J.W. Price, 949/261-8433
Yuichi Futa
S.N. 09/603,632
NAK1-BL53

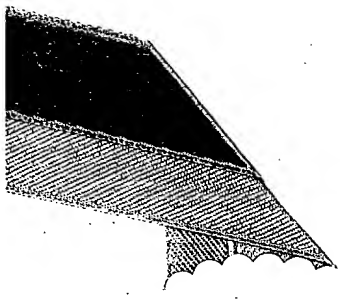
日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

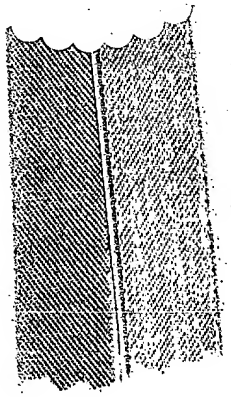
出願年月日
Date of Application: ２０００年　５月１２日

出願番号
Application Number: 特願２０００－１４０８８６

出願人
Applicant (s): 松下電器産業株式会社



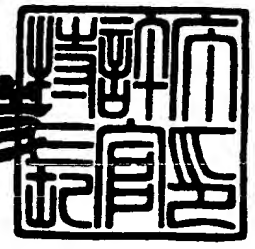
CERTIFIED COPY OF PRIORITY DOCUMENT



２０００年　６月２９日

特許庁長官
Commissioner,
Patent Office

近藤隆彦



【書類名】　特許願
【整理番号】　2022520178
【提出日】　平成12年 5月12日
【あて先】　特許庁長官　殿
【国際特許分類】　G09C　5/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　布田　裕一
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【選任した代理人】
　【識別番号】　100109210
　【弁理士】
　【氏名又は名称】　新居　広守
【先の出願に基づく優先権主張】
　【出願番号】　平成11年特許願第203055号
　【出願日】　平成11年 7月16日
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9810105

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　有限体上の連立方程式求解装置及び逆元演算装置

【特許請求の範囲】

【請求項１】　有限体ＧＦ（ｐ）（ｐは素数）上のｎ元連立一次方程式Ａｘ＝ｂ（ｎは正の整数、Ａはｎ行ｎ列の成分からなる係数行列、ｘはｎ個の成分からなる変数ベクトル、ｂはｎ個の成分からなる定数ベクトル）の解を求める連立方程式求解装置であって、

係数行列Ａと定数ベクトルｂとを記憶しているパラメタ記憶手段と、

前記パラメタ記憶手段から係数行列Ａと定数ベクトルｂとを読み出し、読み出した係数行列Ａ及び定数ベクトルｂを三角化変換して方程式Ａｘ＝ｂと同値の関係を有するｎ元連立一次方程式Ｃｘ＝ｄの係数行列Ｃ（Ｃはｎ行ｎ列の成分からなる係数行列）及び定数ベクトルｄ（ｄはｎ個の成分からなる定数ベクトル）を生成する三角化変換手段と、

前記三角化変換は、係数行列Ａの各対角成分を１に変換しない、係数行列Ａの上三角行列への変換であり、

生成された係数行列Ｃの各対角成分の有限体ＧＦ（ｐ）上の逆元である対角逆元を生成する対角逆元演算手段と、

生成された係数行列Ｃと定数ベクトルｄと生成された各対角逆元とを用いて、方程式Ａｘ＝ｂの解として、方程式Ｃｘ＝ｄの解を求める方程式求解手段と

を備えることを特徴とする連立方程式求解装置。

【請求項２】　前記三角化変換手段は、連続する１個以上の変換過程を介して前記方程式Ｃｘ＝ｄの係数行列Ｃ及び定数ベクトルｄを生成し、

前記各変換過程において、前記三角化変換手段は、変換前のｎ元連立一次方程式から、変換前のｎ元連立一次方程式と同値の関係を有する変換後のｎ元連立一次方程式の係数行列及び定数ベクトルを生成し、最初の変換過程において、変換前のｎ元連立一次方程式は、方程式Ａｘ＝ｂであり、最後の変換過程において、変換後のｎ元連立一次方程式は、方程式Ｃｘ＝ｄであり、

前記各変換過程において、前記変換前のｎ元連立一次方程式は、変換の対象となる１個以上のｎ元一次方程式である対象方程式と、変換の軸となるｎ元一次方

程式である軸方程式とを含み、

前記三角化変換手段は、前記各変換過程において、前記各対象方程式を、前記対象方程式と同値の関係を有する同値方程式に変換する場合に、

第１係数群と第２係数群とを定め、

ここで、前記第１係数群と前記第２係数群とは、それぞれ軸方程式に係る１個以上の値を含む群であり、前記対象方程式において、各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引くことにより、前記対象方程式において０でない係数を有する最高次の変数の係数が０となる前記同値方程式が得られ、

前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし、

前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引く

ことを特徴とする請求項１に記載の連立方程式求解装置。

【請求項３】　前記三角化変換手段は、前記各変換過程において、１個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、

前記三角化変換手段は、各副変換過程において、

軸方程式の０でない係数を有する最高次の変数の係数から構成される群を第１係数群と定め、

軸方程式の各係数及び定数のそれぞれに対象方程式の０でない係数を有する最高次の変数の係数を乗じ、得られた各値から構成される群を第２係数群と定め、

前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし、

前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引く

ことを特徴とする請求項２に記載の連立方程式求解装置。

【請求項４】　前記三角化変換手段は、前記各変換過程において、１個の係数

群算出過程と、前記係数群算出過程後に１個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、

前記係数群算出過程において、前記三角化変換手段は、軸方程式及び１個以上の対象方程式の０でない係数を有する最高次の変数の各係数について、前記各係数を除く他の係数を乗じることにより得られる２個以上の値から構成される群を第１係数群と定め、

前記第１係数群に含まれる値であって、軸方程式の０でない係数を有する最高次の変数の係数を除く他の係数を乗じることにより得られる値と、軸方程式の各係数及び定数とをそれぞれ乗じ、得られた１個以上の値から構成される群を第２係数群と定め、

前記副変換過程において、前記三角化変換手段は、

前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし、

前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引く

ことを特徴とする請求項２に記載の連立方程式求解装置。

【請求項５】　係数行列Ｃの対角成分をm_i（ｉ＝１、２、．．．．、ｎ）とし、対角成分m_iのＧＦ（ｐ）上の対角逆元をI_i（ｉ＝１、２、．．．．、ｎ）とし、

前記対角逆元演算手段は、

【数１】

$$t_i = \prod_{k=1}^{n} m_k \quad (m_i \text{ を除く}) \bmod p$$

$$(i = 1、2、．．．、n)$$

を算出し、

【数２】

$$t = \prod_{k=1}^{n} m_k \mod p$$

を算出する乗算部と、

$u = 1 / t \mod p$

を算出する第１逆元演算部と、

対角逆元 $I_i = u \times t_i \mod p \quad (i = 1、2、\ldots、n)$

を算出する第２逆元演算部と

を含むことを特徴とする請求項３～４のいずれかに記載の連立方程式求解装置

。

【請求項６】　前記乗算部は、

$s_1 = m_1 \times m_2 \mod p$、

$s_2 = s_1 \times m_3 \mod p$、

・・・

$s_{n-3} = s_{n-4} \times m_{n-2} \mod p$

をこの順序で算出し、

次に、

$t_n = s_{n-3} \times m_{n-1} \mod p$

$t_{n-1} = s_{n-3} \times m_n \mod p$

$s_n = m_{n-1} \times m_n \mod p$

$t_{n-2} = s_{n-4} \times s_n \mod p$

$s_{n-1} = m_{n-2} \times s_n \mod p$

$t_{n-3} = s_{n-5} \times s_{n-1} \mod p$

$s_{n-2} = m_{n-3} \times s_{n-1} \mod p$

$t_{n-4} = s_{n-6} \times s_{n-2} \mod p$

・・・

$s_5 = m_4 \times s_6 \mod p$

$t_3 = s_1 \times s_5 \mod p$

$s_4 = m_3 \times s_5 \mod p$

$t_2 = m_1 \times s_4 \mod p$

$t_1 = m_2 \times s_4 \mod p$

をこの順序で算出し、

次に、正の整数の集合｛１、２、．．．．、ｎ｝から選択された１個の値ｊについて、

$t = t_j \times m_j$

を算出する

ことを特徴とする請求項５に記載の連立方程式求解装置。

【請求項７】　有限体ＧＦ（ｐ）（ｐは素数）の拡大体ＧＦ（ｑ）（$q = p^n$、ｎは正の整数）の元ｘの逆元Ｉを演算する逆元演算装置であって、

元ｘと拡大体ＧＦ（ｐ）上の多項式の係数とを用いて、ｎ元連立一次方程式Ａｙ＝Ｂの係数行列Ａ及び定数ベクトルＢを生成する方程式生成手段と、

請求項１～６のいずれかに記載の連立方程式求解装置であって、ｎ元連立一次方程式Ａｙ＝Ｂの解を求める方程式演算手段と、

前記根と求められた前記解とを用いて、逆元Ｉを算出する逆元算出手段と

を備えることを特徴とする逆元演算装置。

【請求項８】　有限体ＧＦ（ｐ）（ｐは素数）の拡大体ＧＦ（ｑ）（$q = p^n$、ｎは正の整数）の上の楕円曲線をＥ、楕円曲線Ｅのベースポイントをｇとし、楕円曲線Ｅ上の離散対数問題を安全性の根拠として利用して安全性を確保する通信を行い、安全性の確保に際して拡大体ＧＦ（ｑ）上の元ｘの逆元Ｉを算出する通信システムであって、

元ｘと拡大体ＧＦ（ｐ）上の多項式の係数とを用いて、ｎ元連立一次方程式Ａｙ＝Ｂの係数行列Ａ及び定数ベクトルＢを生成する方程式生成手段と、

請求項１～６のいずれかに記載の連立方程式求解装置であって、ｎ元連立一次方程式Ａｙ＝Ｂの解を求める方程式演算手段と、

前記根と求められた前記解とを用いて、逆元Ｉを算出する逆元算出手段と

を備えることを特徴とする通信システム。

【請求項９】　有限体ＧＦ（ｐ）（ｐは素数）の拡大体ＧＦ（ｑ）（ｑ＝p^n、ｎは正の整数）の上の楕円曲線をＥ、楕円曲線Ｅのベースポイントをｇとし、楕円曲線Ｅ上の離散対数問題を安全性の根拠として暗号化されたデジタル著作物を記録している記録媒体から暗号化デジタル著作物を読み出して復号し、復号に際して拡大体ＧＦ（ｑ）上の元ｘの逆元Ｉを算出する記録媒体再生装置であって、

元ｘと拡大体ＧＦ（ｐ）上の多項式の係数とを用いて、ｎ元連立一次方程式Ａｙ＝Ｂの係数行列Ａ及び定数ベクトルＢを生成する方程式生成手段と、

請求項１～６のいずれかに記載の連立方程式求解装置であって、ｎ元連立一次方程式Ａｙ＝Ｂの解を求める方程式演算手段と、

前記根と求められた前記解とを用いて、逆元Ｉを算出する逆元算出手段と

を備えることを特徴とする記録媒体再生装置。

【請求項１０】　有限体ＧＦ（ｐ）（ｐは素数）上のｎ元連立一次方程式Ａｘ＝ｂ（ｎは正の整数、Ａはｎ行ｎ列の成分からなる係数行列、ｘはｎ個の成分からなる変数ベクトル、ｂはｎ個の成分からなる定数ベクトル）の解を求め、係数行列Ａと定数ベクトルｂとを記憶しているパラメタ記憶手段を備える連立方程式求解装置において用いられる連立方程式求解方法であって、

前記パラメタ記憶手段から係数行列Ａと定数ベクトルｂとを読み出し、読み出した係数行列Ａ及び定数ベクトルｂを三角化変換して方程式Ａｘ＝ｂと同値の関係を有するｎ元連立一次方程式Ｃｘ＝ｄの係数行列Ｃ（Ｃはｎ行ｎ列の成分からなる係数行列）及び定数ベクトルｄ（ｄはｎ個の成分からなる定数ベクトル）を生成する三角化変換ステップと、

前記三角化変換は、係数行列Ａの各対角成分を１に変換しない、係数行列Ａの上三角行列への変換であり、

生成された係数行列Ｃの各対角成分の有限体ＧＦ（ｐ）上の逆元である対角逆元を生成する対角逆元演算ステップと、

生成された係数行列Ｃと定数ベクトルｄと生成された各対角逆元とを用いて、方程式Ａｘ＝ｂの解として、方程式Ｃｘ＝ｄの解を求める方程式求解ステップと

を含むことを特徴とする連立方程式求解方法。

【請求項１１】　前記三角化変換ステップは、連続する１個以上の変換過程を介して前記方程式Ｃｘ＝ｄの係数行列Ｃ及び定数ベクトルｄを生成し、

前記各変換過程において、前記三角化変換ステップは、変換前のｎ元連立一次方程式から、変換前のｎ元連立一次方程式と同値の関係を有する変換後のｎ元連立一次方程式の係数行列及び定数ベクトルを生成し、最初の変換過程において、変換前のｎ元連立一次方程式は、方程式Ａｘ＝ｂであり、最後の変換過程において、変換後のｎ元連立一次方程式は、方程式Ｃｘ＝ｄであり、

前記各変換過程において、前記変換前のｎ元連立一次方程式は、変換の対象となる１個以上のｎ元一次方程式である対象方程式と、変換の軸となるｎ元一次方程式である軸方程式とを含み、

前記三角化変換ステップは、前記各変換過程において、前記各対象方程式を、前記対象方程式と同値の関係を有する同値方程式に変換する場合に、

第１係数群と第２係数群とを定め、

ここで、前記第１係数群と前記第２係数群とは、それぞれ軸方程式に係る１個以上の値を含む群であり、前記対象方程式において、各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引くことにより、前記対象方程式において０でない係数を有する最高次の変数の係数が０となる前記同値方程式が得られ、

前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし、

前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引く

ことを特徴とする請求項１０に記載の連立方程式求解方法。

【請求項１２】　前記三角化変換ステップは、前記各変換過程において、１個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、

前記三角化変換ステップは、各副変換過程において、

軸方程式の０でない係数を有する最高次の変数の係数から構成される群を第１係数群と定め、

軸方程式の各係数及び定数のそれぞれに対象方程式の０でない係数を有する最高次の変数の係数を乗じ、得られた各値から構成される群を第２係数群と定め、

前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし、

前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引く

ことを特徴とする請求項１１に記載の連立方程式求解方法。

【請求項１３】　前記三角化変換ステップは、前記各変換過程において、１個の係数群算出過程と、前記係数群算出過程後に１個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、

前記係数群算出過程において、前記三角化変換ステップは、軸方程式及び１個以上の対象方程式の０でない係数を有する最高次の変数の各係数について、前記各係数を除く他の係数を乗じることにより得られる２個以上の値から構成される群を第１係数群と定め、

前記第１係数群に含まれる値であって、軸方程式の０でない係数を有する最高次の変数の係数を除く他の係数を乗じることにより得られる値と、軸方程式の各係数及び定数とをそれぞれ乗じ、得られた１個以上の値から構成される群を第２係数群と定め、

前記副変換過程において、前記三角化変換ステップは、

前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし、

前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引く

ことを特徴とする請求項１１に記載の連立方程式求解方法。

【請求項１４】　係数行列Ｃの対角成分をm_i（ｉ＝１、２、．．．．、ｎ）とし、対角成分m_iのＧＦ（ｐ）上の対角逆元をI_i（ｉ＝１、２、．．．．、ｎ）とし、

前記対角逆元演算ステップは、

【数３】

$$t_i = \prod_{k=1}^{n} m_k \quad (m_i \text{を除く}) \bmod p$$

$$(i = 1、2、\ldots、n)$$

を算出し、

【数４】

$$t = \prod_{k=1}^{n} m_k \bmod p$$

を算出する乗算部と、

$u = 1 / t \bmod p$

を算出する第１逆元演算部と、

対角逆元 $I_i = u \times t_i \bmod p \quad (i = 1、2、\ldots、n)$

を算出する第２逆元演算部と

を含むことを特徴とする請求項１２～１３のいずれかに記載の連立方程式求解方法。

【請求項１５】　前記乗算部は、

$s_1 = m_1 \times m_2 \bmod p$、

$s_2 = s_1 \times m_3 \bmod p$、

・・・

$s_{n-3} = s_{n-4} \times m_{n-2} \bmod p$

をこの順序で算出し、

次に、

$t_n = s_{n-3} \times m_{n-1} \bmod p$

$t_{n-1} = s_{n-3} \times m_n \mod p$

$s_n = m_{n-1} \times m_n \mod p$

$t_{n-2} = s_{n-4} \times s_n \mod p$

$s_{n-1} = m_{n-2} \times s_n \mod p$

$t_{n-3} = s_{n-5} \times s_{n-1} \mod p$

$s_{n-2} = m_{n-3} \times s_{n-1} \mod p$

$t_{n-4} = s_{n-6} \times s_{n-2} \mod p$

・・・

$s_5 = m_4 \times s_6 \mod p$

$t_3 = s_1 \times s_5 \mod p$

$s_4 = m_3 \times s_5 \mod p$

$t_2 = m_1 \times s_4 \mod p$

$t_1 = m_2 \times s_4 \mod p$

をこの順序で算出し、

次に、正の整数の集合｛１、２、・・・、ｎ｝から選択された１個の値ｊについて、

$t = t_j \times m_j$

を算出する

ことを特徴とする請求項１４に記載の連立方程式求解方法。

【請求項１６】　有限体ＧＦ（ｐ）（ｐは素数）上のｎ元連立一次方程式Ａｘ＝ｂ（ｎは正の整数、Ａはｎ行ｎ列の成分からなる係数行列、ｘはｎ個の成分からなる変数ベクトル、ｂはｎ個の成分からなる定数ベクトル）の解を求め、係数行列Ａと定数ベクトルｂとを記憶しているパラメタ記憶手段を備えるコンピュータで用いられる連立方程式求解プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、

前記プログラムは、

前記パラメタ記憶手段から係数行列Ａと定数ベクトルｂとを読み出し、読み出した係数行列Ａ及び定数ベクトルｂを三角化変換して方程式Ａｘ＝ｂと同値の関係を有するｎ元連立一次方程式Ｃｘ＝ｄの係数行列Ｃ（Ｃはｎ行ｎ列の成分から

なる係数行列）及び定数ベクトルｄ（ｄはｎ個の成分からなる定数ベクトル）を生成する三角化変換ステップと、

前記三角化変換は、係数行列Ａの各対角成分を１に変換しない、係数行列Ａの上三角行列への変換であり、

生成された係数行列Ｃの各対角成分の有限体ＧＦ（ｐ）上の逆元である対角逆元を生成する対角逆元演算ステップと、

生成された係数行列Ｃと定数ベクトルｄと生成された各対角逆元とを用いて、方程式Ａｘ＝ｂの解として、方程式Ｃｘ＝ｄの解を求める方程式求解ステップとを含むことを特徴とする記録媒体。

【請求項１７】　前記三角化変換ステップは、連続する１個以上の変換過程を介して前記方程式Ｃｘ＝ｄの係数行列Ｃ及び定数ベクトルｄを生成し、

前記各変換過程において、前記三角化変換ステップは、変換前のｎ元連立一次方程式から、変換前のｎ元連立一次方程式と同値の関係を有する変換後のｎ元連立一次方程式の係数行列及び定数ベクトルを生成し、最初の変換過程において、変換前のｎ元連立一次方程式は、方程式Ａｘ＝ｂであり、最後の変換過程において、変換後のｎ元連立一次方程式は、方程式Ｃｘ＝ｄであり、

前記各変換過程において、前記変換前のｎ元連立一次方程式は、変換の対象となる１個以上のｎ元一次方程式である対象方程式と、変換の軸となるｎ元一次方程式である軸方程式とを含み、

前記三角化変換ステップは、前記各変換過程において、前記各対象方程式を、前記対象方程式と同値の関係を有する同値方程式に変換する場合に、

第１係数群と第２係数群とを定め、

ここで、前記第１係数群と前記第２係数群とは、それぞれ軸方程式に係る１個以上の値を含む群であり、前記対象方程式において、各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引くことにより、前記対象方程式において０でない係数を有する最高次の変数の係数が０となる前記同値方程式が得られ、

前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし

前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引く

ことを特徴とする請求項１７に記載の記録媒体。

【請求項１８】　前記三角化変換ステップは、前記各変換過程において、１個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、

前記三角化変換ステップは、各副変換過程において、

軸方程式の０でない係数を有する最高次の変数の係数から構成される群を第１係数群と定め、

軸方程式の各係数及び定数のそれぞれに対象方程式の０でない係数を有する最高次の変数の係数を乗じ、得られた各値から構成される群を第２係数群と定め、

前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし

、

前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引く

ことを特徴とする請求項１７に記載の記録媒体。

【請求項１９】　前記三角化変換ステップは、前記各変換過程において、１個の係数群算出過程と、前記係数群算出過程後に１個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、

前記係数群算出過程において、前記三角化変換ステップは、軸方程式及び１個以上の対象方程式の０でない係数を有する最高次の変数の各係数について、前記各係数を除く他の係数を乗じることにより得られる２個以上の値から構成される群を第１係数群と定め、

前記第１係数群に含まれる値であって、軸方程式の０でない係数を有する最高次の変数の係数を除く他の係数を乗じることにより得られる値と、軸方程式の各係数及び定数とをそれぞれ乗じ、得られた１個以上の値から構成される群を第２係数群と定め、

前記副変換過程において、前記三角化変換ステップは、

前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし

、

前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引く

ことを特徴とする請求項１７に記載の記録媒体。

【請求項２０】　係数行列Ｃの対角成分をm_i（ｉ＝１、２、．．．、ｎ）とし、対角成分m_iのＧＦ（ｐ）上の対角逆元をI_i（ｉ＝１、２、．．．、ｎ）とし、

前記対角逆元演算ステップは、

【数５】

$$t_i = \prod_{k=1}^{n} m_k \ (m_i \text{を除く}) \bmod p \quad (i=1、2、...、n)$$

を算出し、

【数６】

$$t = \prod_{k=1}^{n} m_k \bmod p$$

を算出する乗算部と、

$u = 1 / t \bmod p$

を算出する第１逆元演算部と、

対角逆元$I_i = u \times t_i \bmod p$　（ｉ＝１、２、．．．、ｎ）

を算出する第２逆元演算部と

を含むことを特徴とする請求項１８～１９のいずれかに記載の記録媒体。

【請求項２１】　前記乗算部は、

$s_1 = m_1 \times m_2 \mod p$、

$s_2 = s_1 \times m_3 \mod p$、

・・・

$s_{n-3} = s_{n-4} \times m_{n-2} \mod p$

をこの順序で算出し、

次に、

$t_n = s_{n-3} \times m_{n-1} \mod p$

$t_{n-1} = s_{n-3} \times m_n \mod p$

$s_n = m_{n-1} \times m_n \mod p$

$t_{n-2} = s_{n-4} \times s_n \mod p$

$s_{n-1} = m_{n-2} \times s_n \mod p$

$t_{n-3} = s_{n-5} \times s_{n-1} \mod p$

$s_{n-2} = m_{n-3} \times s_{n-1} \mod p$

$t_{n-4} = s_{n-6} \times s_{n-2} \mod p$

・・・

$s_5 = m_4 \times s_6 \mod p$

$t_3 = s_1 \times s_5 \mod p$

$s_4 = m_3 \times s_5 \mod p$

$t_2 = m_1 \times s_4 \mod p$

$t_1 = m_2 \times s_4 \mod p$

をこの順序で算出し、

次に、正の整数の集合｛１、２、・・・・、ｎ｝から選択された１個の値ｊについて、

$t = t_j \times m_j$

を算出する

ことを特徴とする請求項２０に記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報セキュリテイ技術としての暗号技術及び誤り訂正技術に関し、特に、拡大体及び連立方程式を用いる演算技術に関する。

【０００２】

【従来の技術】

近年、秘密通信方式やデジタル署名方式による通信が用いられるようになっている。

秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行なう方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、本人であることを証明する通信方式である。この署名方式には公開鍵暗号方式と呼ばれる暗号方式を用いる。公開鍵暗号方式は通信相手が多数の時、通信相手ごとに異なる暗号鍵を容易に管理するための方式であり、多数の通信相手と通信を行なうのに不可欠な基盤技術である。

【０００３】

公開鍵暗号方式では、暗号化鍵と復号化鍵とが異なり、復号化鍵を秘密にし、暗号化鍵を公開する。この公開鍵暗号方式の安全性の根拠として離散対数問題が用いられる。離散対数問題には代表的なものとして、有限体上定義されるもの及び楕円曲線上定義されるものがある。離散対数問題については、「A Course in Number theory and Cryptography」（Neal Koblitz著、Springer-Verlag,1987）に詳しく述べられている。

（楕円曲線上の離散対数問題）

楕円曲線上の離散対数問題とは、

Ｅを有限体ＧＦ（ｑ）（$q=p^n$、ｐは素数、ｎは正の整数）上定義された楕円曲線とし、楕円曲線Ｅの位数が大きな素数で割り切れるとき、楕円曲線Ｅ上の元Ｇをベースポイントとする。このとき、楕円曲線Ｅ上の与えられた元Ｙに対して、

$$Y=x*G$$

となる整数ｘが存在するならば、ｘを求めよ、という問題である。

【０００４】

なお、この明細書において、演算子＊は、楕円曲線上の加算を意味し、ｘ＊Ｇ

は、楕円曲線上でＧをｘ回加算することを示す。また、ＧＦ（ｑ）はＧＦ（ｐ）の拡大体である。拡大体については、「現代暗号」（岡本龍明、山本博資著、シリーズ／情報科学の数学、産業図書、1997、26～28ページ）に詳しく述べられている。

（従来例１：楕円曲線上の離散対数問題を応用するエルガマル署名）

次に、楕円曲線上の離散対数問題を応用するエルガマル署名について、図９に示すシーケンス図を用いて説明する。

【０００５】

ユーザＡが使用する装置（以下、ユーザＡ３１０と称する。）、管理センタにおいて使用される装置（以下、管理センタ３２０と称する。）及びユーザＢが使用する装置（以下、ユーザＢ３３０と称する。）は、それぞれネットワークで接続されている。

ｐを素数、$q=p^n$、ｎは正の整数、有限体ＧＦ（ｑ）上の楕円曲線をＥとする。楕円曲線Ｅのベースポイントをとし、Ｇの位数をｒとする。すなわち、ｒは、

$r*G=0$

を満たす最小の正整数である。ここで、０は楕円曲線の群の加算における零元である。

【０００６】

（１）管理センタ３２０による公開鍵の生成

管理センタ３２０は、ユーザＡ３１０からユーザＡ３１０が秘密に所有する秘密鍵x_Aを予め通知されており（ステップＳ１）、秘密鍵x_Aを用いて、次の式より、ユーザＡ３１０の公開鍵Y_Aを作成する（ステップＳ２）。

$Y_A=x_A*G$

その後、管理センタ３２０は、有限体ＧＦ（ｑ）、楕円曲線Ｅ及びベースポイントＧをシステムパラメータとして公開し、ユーザＢ３３０にユーザＡ３１０の公開鍵Y_Aを公開する（ステップＳ３～Ｓ４）。

【０００７】

（２）ユーザＡ３１０による署名生成

ユーザＡ３１０は、乱数ｋを生成する（ステップＳ５）。次に、ユーザＡ３１０は、

$R_1 = (r_x, r_y) = k * G$

を計算し（ステップＳ６）、

$s \times k = m + r_x \times x_A \mod r$

から、ｓを計算する（ステップＳ７）。ここで、ｍは、ユーザＡ３１０がユーザＢ３３０へ送信するメッセージである。

【０００８】

さらに、ユーザＡ３１０は、得られた（R_1、ｓ）を署名としてメッセージｍとともに、ユーザＢ３３０へ送信する（ステップＳ８）。

（３）ユーザＢ３３０による署名検証

ユーザＢ３３０は、

$s * R_1 = m * G + r_x * Y_A$

が成立するかどうか判定することにより、送信者であるユーザＡ３１０の身元を確認する（ステップＳ９）。これは、

$$s * R_1 = [((m + r_x \times x_A) / k) \times k] * G$$
$$= (m + r_x \times x_A) * G$$
$$= m * G + (r_x \times x_A) * G$$
$$= m * G + r_x * Y_A$$

となることから明らかである。

【０００９】

上記に示した楕円曲線上の離散対数問題を応用するエルガマル署名によるデジタル署名方式における公開鍵の生成、署名生成及び署名検証のそれぞれにおいて、楕円曲線上の点の冪倍の演算が行われる。

楕円曲線の演算公式については、

「Efficient elliptic curve exponentiation」（Miyaji, Ono, and Cohen著、Advances in cryptology-proceedings of ICICS'97, Lecture notes in computer science, 1997, Springer-verlag, 282-290.）に詳しく説明されている。

【００１０】

楕円曲線の方程式を

$y^2 = x^3 + a \times x + b$

とする。楕円曲線上の任意の点Ｐの座標を（x_1、y_1）とする。この座標はアフィン座標と呼ばれている。

楕円曲線上における加算には、有限体ＧＦ（ｑ）の逆元演算の処理を含むことが知られている。上記の論文では、射影座標と呼ばれる座標に触れているが、これは、

（x_1、y_1）→　（x_1、y_1、１）

のように、２項組座標を３項組座標に対応づけるものである。３項組座標の場合、楕円曲線の加算には、有限体ＧＦ（ｑ）の逆元演算の処理が含まれない。一般に有限体の逆元演算は、計算時間が長いため、３項組座標がよく用いられる。

【００１１】

逆に、

（Ｘ、Ｙ、Ｚ）→　（Ｘ／Ｚ、Ｙ／Ｚ）

のように、２項組座標は３項組座標に対応づけられる。ここで、逆元演算が必要となる。

上記のエルガマル署名のステップＳ６においては、２項組座標を３項組座標に変換し、３項組座標により楕円曲線上の加算を行い、加算結果の３項組座標をアフィン座標に変換する。したがって、３項組座標からアフィン座標への変換において、逆元演算が必要になる。

（従来例２：拡大体上の逆元演算）

以下において、従来の拡大体ＧＦ（ｑ）（$q = p^n$、ｐは素数、ｎは正の整数）の逆元演算について説明する。

【００１２】

ここで、簡単のため、拡大体ＧＦ（ｑ）の生成多項式をｆ（ｇ）$= g^n - \beta$とし、生成多項式の根をαとし、生成多項式の入力となるＧＦ（ｑ）の元を

$x = x_0 + x_1 \times \alpha + \cdots + x_{n-1} \times \alpha^{n-1}$ とする。

（１）ステップ１

ＧＦ（ｑ）の元ｘを基にして、y_i（$0 \leqq i \leqq n-1$）に関する以下の連立方

程式を生成する。

【００１３】

$$x_0 y_0 + \beta x_{n-1} y_1 + \beta x_{n-2} y_2 + \cdots + \beta x_1 y_{n-1} = 1$$
$$x_1 y_0 + x_0 y_1 + \beta x_{n-1} y_2 + \cdots + \beta x_2 y_{n-1} = 0$$
$$x_2 y_0 + x_1 y_1 + x_0 y_2 + \cdots + \beta x_3 y_{n-1} = 0$$
$$\cdots$$
$$x_{n-2} y_0 + x_{n-3} y_1 + x_{n-4} y_2 + \cdots + \beta x_{n-1} y_{n-1} = 0$$
$$x_{n-1} y_0 + x_{n-2} y_1 + x_{n-3} y_2 + \cdots + x_0 y_{n-1} = 0$$

（２）ステップ２

生成された連立方程式の解y_k（ｋ＝０、１、・・・、ｎ－１）を求める。

（３）ステップ３

求めた解y_k（ｋ＝０、１、・・・、ｎ－１）を

逆元$I = y_0 + y_1 \alpha + \cdots + y_{n-1} \alpha^{n-1}$に変換する。

【００１４】

このようにして、拡大体ＧＦ（ｑ）上の元の逆元が求められる。

次に、上記のようにして逆元演算ができる根拠について説明する。

上記の逆元Ｉと元ｘについて、

$xI = 1 \mod f(g)$

という関係を満たすとき、

$$xI = x_0 (y_0 + y_1 \alpha + \cdots + y_{n-1} \alpha^{n-1})$$
$$+ x_1 \alpha (y_0 + y_1 \alpha + \cdots + y_{n-1} \alpha^{n-1})$$
$$+ x_2 \alpha^2 (y_0 + y_1 \alpha + \cdots + y_{n-1} \alpha^{n-1})$$
$$\cdots$$
$$+ x_{n-1} \alpha^{n-1} (y_0 + y_1 \alpha + \cdots + y_{n-1} \alpha^{n-1})$$

であり、

$\alpha^n = \beta \mod f(g)$

であるので、

$$xI = x_0 (y_0 + y_1 \alpha + \cdots + y_{n-1} \alpha^{n-1})$$
$$+ x_1 (y_0 \alpha + y_1 \alpha^2 + \cdots + y_{n-1} \beta)$$

$$+x_2\ (y_0\ \alpha^2+y_1\ \alpha^3+\cdots+y_{n-1}\ \alpha\beta)$$
$$\cdots$$
$$+x_{n-1}\ (y_0\ \alpha^{n-1}+y_1\ \beta+\cdots+y_{n-1}\ \alpha^{n-2}\ \beta)$$

であり、αの降冪の順に整理すると

$$xI=x_0\ y_0+\beta\times x_{n-1}\times y_1+\cdots+\beta\ x_1\ y_{n-1}$$
$$+\alpha\ (x_1\ y_0+x_0\times y_1+\cdots+\beta\ x_2\ y_{n-1})$$
$$+\alpha^2\ (x_2\ y_0+x_1\ y_1+\cdots+\beta\ x_3\ y_{n-1})$$
$$\cdots$$
$$+\alpha^{n-1}\ (x_{n-1}\ y_0+x_{n-2}\ y_1+\cdots+x_0\ y_{n-1})$$

である。

【００１５】

ここで、ｘＩが１に等しいので、上記ステップ１において生成された連立方程式を導くことができる。

したがって、拡大体ＧＦ（ｑ）の逆元を求めることは、基礎体ＧＦ（ｐ）上の連立方程式を解くことと等しい。

また、上記例では、$g^n-\beta$の形の生成多項式を扱ったが、一般の生成多項式に対しても同様の操作により、方程式を生成できる。

（従来例３：基礎体ＧＦ（ｐ）上の連立方程式の解法）

以下において、基礎体ＧＦ（ｐ）上の連立方程式の従来の解法について説明する。この解法は、ガウスの消去法と呼ばれる。ガウスの消去法については、「コンピュータによる数値計算」（水上孝一編著、プログラミング入門シリーズ、朝倉書店、1985、76～82ページ）に詳しく述べられている。

【００１６】

x_k（ｋ＝０、１、２、・・・、ｎ－１）に対する連立方程式を、

$$a_{11}x_0+a_{12}x_1+\cdots+a_{1n}x_{n-1}=b_1$$
$$a_{21}x_0+a_{22}x_1+\cdots+a_{2n}x_{n-1}=b_2$$
$$\cdots$$
$$a_{n1}x_0+a_{n2}x_1+\cdots+a_{nn}x_{n-1}=b_n$$

とし、この解を求める。

（ステップ１）

行列M、ベクトルｖを以下のようにおく。

【００１７】

【数７】

$$M=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

$$v=\begin{pmatrix} b_1 \\ b_2 \\ \cdot \\ \cdot \\ b_n \end{pmatrix}$$

【００１８】

また、ベクトルＸを次のようにおく。

【００１９】

【数８】

$$X=\begin{pmatrix} x_0 \\ x_1 \\ \cdot \\ \cdot \\ x_{n-1} \end{pmatrix}$$

【００２０】

上記の連立方程式は、次のように表現できる。

ＭＸ＝ｖ

行列Ｍを三角化するように、行列M、ベクトルｖを変換し、それぞれ行列M'

、ベクトルｖ’を生成する。ここで、三角化とは、行列の対角成分より下の成分がすべて０となるような変換をいう。また、このような行列を上三角行列と呼ぶ。

【００２１】

次に上記の従来の三角化の手順について、図１０に示すフローチャートを用いて説明する。

カウンタｊに１を設定する（ステップＳ２１）。次に、a_{jj}の逆元I_jを算出し（ステップＳ２２）、a_{jj}に１を設定し（ステップＳ２３）、$j+1 \leqq k \leqq n$に対して、$a_{jk}=a_{jk} \times I_j$、$b_j=b_j \times I_j$とする（ステップＳ２４）。次にカウンタｉ＝カウンタｊ＋１とする（ステップＳ２５）。

【００２２】

a_{ij}に０を設定し（ステップＳ２６）、$j+1 \leqq k \leqq n$に対して、$a_{ik}=a_{ik}-a_{jj} \times a_{jk}$とし（ステップＳ２７）、$b_i=b_i-a_{ij} \times b_j$とする（ステップＳ２８）。次に、ｉ＝ｎであるか否かを判断し、ｉ＝ｎでなければ（ステップＳ２９）、カウンタｉに１を加算して（ステップＳ３１）、制御をステップＳ２６へ戻す。ｉ＝ｎであれば（ステップＳ２９）、ｊ＝ｎであるか否かを判断し、ｊ＝ｎでなければ（ステップＳ３０）、カウンタｊに１を加算して（ステップＳ３２）、制御をステップＳ２２へ戻す。ｊ＝ｎであれば（ステップＳ３０）、処理を終了する。

【００２３】

このようにして得られた行列をＭ’、ベクトルをｖ’とする。ここで、行列Ｍ’の対角成分は１であり、行列Ｍ’の対角成分より下の成分がすべて０である。

連立方程式Ｍ’Ｘ＝ｖ’と、連立方程式ＭＸ＝ｖとは、同値の関係を有する。ここで、

【００２４】

【数９】

$$M' = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{bmatrix}$$

$$v' = \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{bmatrix}$$

【００２５】

とする。

（ステップ２）

生成された行列M’、ベクトルｖ’を用いて、次に示すようにして、連立方程式M’Ｘ＝ｖ’の解を求める。

カウンタｃにｎ－１、・・・、１、０の値をこの順に設定し、カウンタｃの各値について、

ｃ＝ｎ－１のとき、　$y_c = d_{c+1}$

ｃ≠ｎ－１のとき、

【００２６】

【数１０】

$$y_c = d_{c+1} - \sum_{i=c+1}^{n-1} (c_{c+1\ i+1} \times y_{i-1})$$

【００２７】

を算出する。

（具体例）

従来例３を適用する具体例を以下に示す。

なお、この具体例は、三角化変換を分かりやすく説明するための例である。暗号通信システムやデジタル署名システムにおいて実際に使用される例ではないので注意を要する。

【００２８】

素数ｐ＝３１、生成多項式ｆ（ｇ）＝g^5－２、ＧＦ（ｑ）の元ｘ＝５α^4＋２９α^3＋６α^2＋１９α＋１７とする。

$x \times \alpha = 5\alpha^5 + 29\alpha^4 + 6\alpha^3 + 19\alpha^2 + 17\alpha$

$= 29\alpha^4 + 6\alpha^3 + 19\alpha^2 + 17\alpha + 5 \times 2$

$x \times \alpha^2 = 29\alpha^5 + 6\alpha^4 + 19\alpha^3 + 17\alpha^2 + 10\alpha$

$= 6\alpha^4 + 19\alpha^3 + 17\alpha^2 + 10\alpha + 29 \times 2$

$x \times \alpha^3 = 6\alpha^5 + 19\alpha^4 + 17\alpha^3 + 10\alpha^2 + 27\alpha$

$= 19\alpha^4 + 17\alpha^3 + 10\alpha^2 + 27\alpha + 6 \times 2$

$x \times \alpha^4 = 19\alpha^5 + 17\alpha^4 + 10\alpha^3 + 27\alpha^2 + 12\alpha$

$= 17\alpha^4 + 10\alpha^3 + 27\alpha^2 + 12\alpha + 19 \times 2$

であるので、連立方程式は、図１１（ａ）に示すようになる。係数行列３０１は、５行５列の成分からなり、定数ベクトル３０２は、５個の成分からなる。

【００２９】

この連立方程式において、一次方程式

$17x_0 + 10x_1 + 27x_2 + 12x_3 + 7x_4 = 1$

を変換を行う際に軸となる軸方程式と呼び、この連立方程式の他の方程式を変換の対象となる対象方程式と呼ぶ。

次に、逆元演算を行う。

【００３０】

１／１７　ｍｏｄ　３１　＝　１１

続けて、次の演算を行う。

１０×１１　ｍｏｄ　３１　＝　１７

２７×１１　ｍｏｄ　３１　＝　１８

１２×１１　ｍｏｄ　３１　＝　８

７×１１　ｍｏｄ　３１　＝　１５

１×１１　ｍｏｄ　３１　＝　１１

従って、連立方程式は、図１１（ｂ）に示すようになる。ここで、係数行列３１１の１列１行の成分は、１となる。この図の係数行列３１１及び定数ベクトル３１２において、枠で囲まれた数字は、図１１（ａ）に示す係数行列３０１及び定数ベクトル３０２から変化した係数を示す。以下の図においても同様である。

【００３１】

ここで、上記の逆元演算１／１７　ｍｏｄ　３１　＝　１１の詳細について以下に説明する。

この逆元演算においては、

ａ×１７＋ｂ×３１　＝　１

を満たすａを拡張ＧＣＤ法によって求め、ａの値を前記逆元演算の演算値とする。

【００３２】

拡張ＧＣＤ法は、乗算や加算を繰り返し行うため、一般に計算量が多い。

拡張ＧＣＤ法については、「A Course in Computational Algebraic Number Theory」（H. Cohen著、Graduate texts in mathematics 138, 1996, Springer-Verlag,16～19ページ）に説明されている。

次に、係数行列３１１の１列２行の成分がそれぞれ０となるように、

１７－１７×１９＝４　　ｍｏｄ　３１

１０－１８×１９＝９　　ｍｏｄ　３１

２７－　８×１９＝３０　　ｍｏｄ　３１

１２－１５×１９＝６　　ｍｏｄ　３１

　０－１１×１９＝８　　ｍｏｄ　３１

を演算する。同様にして、係数行列３１１の１列３行～５行の成分がそれぞれ０となるように、係数行列３１１を係数行列３２１に変換し、ベクトル３１２をベクトル３２２に変換し、図１１（ｃ）に示す連立方程式が得られる。

【００３３】

次に、行列３２１の２列２行の成分が１となるように、係数行列３２１を係数行列３３１に変換し、ベクトル３２２をベクトル３３２に変換し、図１１（ｄ）

に示す連立方程式が得られる。さらに、前記と同様にして、係数行列３３１の２列３行～５行の成分が０となるように、係数行列３３１を係数行列３４１に変換し、ベクトル３３２をベクトル３４２に変換し、図１１（ｅ）に示す連立方程式が得られる。

【００３４】

以下同様にして、図１１（ｆ）に示す係数行列３５１のように３列３行の成分は１となり、図１１（ｇ）に示す係数行列３６１のように３列４行～５行の成分は０となる。さらに、図１１（ｈ）に示す係数行列３７１のように４列４行の成分は１となり、図１１（ｉ）に示す係数行列３８１のように４列５行の成分は０となる。最後に、図１１（ｊ）に示す係数行列３９１のように５列５行の成分は１となる。

【００３５】

このようにして、係数行列が上三角行列に変換される。

次に、

$y_4 = 29$

$y_3 = 15 - 21 \times 29$

$= 26 \mod 31$

$y_2 = 11 - 4 \times 26 - 28 \times 29$

$= 25 \mod 31$

$y_1 = 2 - 10 \times 25 - 23 \times 26 - 17 \times 29$

$= 25 \mod 31$

$y_0 = 11 - 17 \times 25 - 18 \times 25 - 8 \times 26 - 15 \times 29$

$= 12 \mod 31$

を算出する。

（計算量の評価）

従来例３の全計算量は、次に示すようになる。ここで、基礎体の乗算、逆元演算の計算量をそれぞれ、Mul、Invとする。

【００３６】

上記のステップ１について、カウンタｊに対するループ内の計算量の内訳は次

のようになる。

（ａ）ステップＳ２２において、１回の逆元演算が必要であるので、１Inv

（ｂ）ステップＳ２４において、（ｎ－（ｊ＋１）＋１）＋１＝ｎ－ｊ＋１回の乗算が必要であるので、（ｎ－ｊ＋１）×Mul

（ｃ）カウンタｉが変化する範囲ｊ＋１～ｎにおいて、以下のとおり。

【００３７】

（ｃ－１）　ステップＳ２７において、（ｎ－（ｊ＋１）＋１）回の乗算が必要であるので、（ｎ－ｊ）×Mul

（ｃ－２）　ステップＳ２８において、１回の乗算が必要であるので、１Mul

（ｃ－１）と（ｃ－２）とを（ｎ－（ｊ＋１）＋１）＝（ｎ－ｊ）回行うので、（ｃ）全体では、（ｎ－ｊ）（ｎ－ｊ＋１）×Mulとなる。

【００３８】

次に、（ａ）、（ｂ）、（ｃ）の合計は、（ｎ－ｊ＋１）（ｎ－ｊ＋１）×Mul＋１Inv

カウンタｊは、１～ｎの範囲で変化するので、ステップ１全体の計算量は、

【００３９】

【数１１】

$$\sum_{j=1}^{n}\left((n-j+1)(n-j+1)\times Mul+Inv\right)$$

$$=\sum_{j=1}^{n}(n-j+1)(n-j+1)\times Mul$$

$$+\sum_{j=1}^{n}1\,Inv$$

$$=\sum_{j=1}^{n}j^{2}\times Mul+n\times Inv$$

$$=1/6\times n(n+1)(2n+1)+n\times Inv$$

【００４０】

となる。

上記のステップ２について、計算量は次のようになる。

カウンタｃに対して、（ｎ－（ｃ＋１）＋１）＝（ｎ－ｃ）回の乗算が必要であるので、（ｎ－ｃ）×Mul

カウンタｃは、１～ｎの範囲で変化するので、ステップ２全体の計算量は、

【００４１】

【数１２】

$$\sum_{c=1}^{n} (n-c) \times Mul$$

$$= \sum_{c=1}^{n} (c-1) \times Mul$$

$$= \left(\sum_{c=1}^{n} c - \sum_{c=1}^{n} 1\right) \times Mul$$

$$= (1/2 \times n(n+1) - n) \times Mul$$

$$= 1/2 \times n(n-1) \times Mul$$

【００４２】

従って、従来例３の全体の計算量は、

（１／６×ｎ（ｎ＋１）（２ｎ＋１）＋１／２×ｎ（ｎ－１））×Mul＋ｎ×Inv

＝　１／３×ｎ×（n^2 ＋３ｎ－１）×Mul＋ｎ×Inv

となる。

ここで、ｎ＝５、｜ｑ｜＝１６０（｜ｑ｜はｑのビットサイズ）の場合、一般的な計算機では、Inv ＝４０Mul であることが知られているので、従来例３の全体の計算量は、２６５×Mulである。

【００４３】

【発明が解決しようとする課題】

以上説明したように、有限体上の連立方程式を解くことにより、拡大体上の逆元演算ができるものの、拡大体上の逆元演算の計算量は一般に大きいので、有限体上の連立方程式の求解及び拡大体上の逆元演算における計算量をさらに少なくしたいという要望がある。

【００４４】

本発明は、上記の要望に鑑み、有限体上の連立方程式の求解法において、計算量を削減することができる有限体上の連立方程式の求解装置、求解方法、求解プログラムを記録している記録媒体、拡大体上の逆元演算における計算量を削減することができる拡大体上の逆元演算装置、逆元演算方法、逆元演算プログラムを記録している記録媒体、これらの装置を応用する通信システム及び記録媒体再生装置を提供することを目的とする。

【００４５】

【課題を解決するための手段】

上記の目的を達成するために、本発明は、有限体ＧＦ（ｐ）（ｐは素数）上のｎ元連立一次方程式Ａｘ＝ｂ（ｎは正の整数、Ａはｎ行ｎ列の成分からなる係数行列、ｘはｎ個の成分からなる変数ベクトル、ｂはｎ個の成分からなる定数ベクトル）の解を求める連立方程式求解装置であって、係数行列Ａと定数ベクトルｂとを記憶しているパラメタ記憶手段と、前記パラメタ記憶手段から係数行列Ａと定数ベクトルｂとを読み出し、読み出した係数行列Ａ及び定数ベクトルｂを三角化変換して方程式Ａｘ＝ｂと同値の関係を有するｎ元連立一次方程式Ｃｘ＝ｄの係数行列Ｃ（Ｃはｎ行ｎ列の成分からなる係数行列）及び定数ベクトルｄ（ｄはｎ個の成分からなる定数ベクトル）を生成する三角化変換手段と、前記三角化変換は、係数行列Ａの各対角成分を１に変換しない、係数行列Ａの上三角行列への変換であり、生成された係数行列Ｃの各対角成分の有限体ＧＦ（ｐ）上の逆元である対角逆元を生成する対角逆元演算手段と、生成された係数行列Ｃと定数ベクトルｄと生成された各対角逆元とを用いて、方程式Ａｘ＝ｂの解として、方程式Ｃｘ＝ｄの解を求める方程式求解手段とを備えることを特徴とする。

【００４６】

ここで、前記三角化変換手段は、連続する１個以上の変換過程を介して前記方

程式Ｃｘ＝ｄの係数行列Ｃ及び定数ベクトルｄを生成し、前記各変換過程において、前記三角化変換手段は、変換前のｎ元連立一次方程式から、変換前のｎ元連立一次方程式と同値の関係を有する変換後のｎ元連立一次方程式の係数行列及び定数ベクトルを生成し、最初の変換過程において、変換前のｎ元連立一次方程式は、方程式Ａｘ＝ｂであり、最後の変換過程において、変換後のｎ元連立一次方程式は、方程式Ｃｘ＝ｄであり、前記各変換過程において、前記変換前のｎ元連立一次方程式は、変換の対象となる１個以上のｎ元一次方程式である対象方程式と、変換の軸となるｎ元一次方程式である軸方程式とを含み、前記三角化変換手段は、前記各変換過程において、前記各対象方程式を、前記対象方程式と同値の関係を有する同値方程式に変換する場合に、第１係数群と第２係数群とを定め、ここで、前記第１係数群と前記第２係数群とは、それぞれ軸方程式に係る１個以上の値を含む群であり、前記対象方程式において、各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引くことにより、前記対象方程式において０でない係数を有する最高次の変数の係数が０となる前記同値方程式が得られ、前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし、前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引くように構成してもよい。

【００４７】

ここで、前記三角化変換手段は、前記各変換過程において、１個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、前記三角化変換手段は、各副変換過程において、軸方程式の０でない係数を有する最高次の変数の係数から構成される群を第１係数群と定め、軸方程式の各係数及び定数のそれぞれに対象方程式の０でない係数を有する最高次の変数の係数を乗じ、得られた各値から構成される群を第２係数群と定め、前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし、前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引くように構

成してもよい。

【００４８】

ここで、前記三角化変換手段は、前記各変換過程において、１個の係数群算出過程と、前記係数群算出過程後に１個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、前記係数群算出過程において、前記三角化変換手段は、軸方程式及び１個以上の対象方程式の０でない係数を有する最高次の変数の各係数について、前記各係数を除く他の係数を乗じることにより得られる２個以上の値から構成される群を第１係数群と定め、前記第１係数群に含まれる値であって、軸方程式の０でない係数を有する最高次の変数の係数を除く他の係数を乗じることにより得られる値と、軸方程式の各係数及び定数とをそれぞれ乗じ、得られた１個以上の値から構成される群を第２係数群と定め、前記副変換過程において、前記三角化変換手段は、前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし、前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引くように構成してもよい。

【００４９】

【発明の実施の形態】

１　第１の実施の形態

本発明の１の実施の形態としての逆元演算装置１００について説明する。

１．１　逆元演算装置１００の構成

逆元演算装置１００は、予め与えられた有限体ＧＦ（ｐ）（ｐは素数）の拡大体ＧＦ（ｑ）（$q=p^n$、ｎは正の整数）上の元ｘの逆元Ｉを算出する。以下において、拡大体ＧＦ（ｑ）の生成多項式を$g^n-\beta$とし、その根をαとし、元ｘを$x=x_0+x_1\alpha+\cdots+x_{n-1}\alpha^{n-1}$とする。ここで、$\alpha$は、ＧＦ（ｑ）上の元であり、$\beta$、$x_0$、$x_1$、・・・、$x_{n-1}$は、ＧＦ（ｐ）上の元である。

【００５０】

逆元演算装置１００は、図１に示すように、パラメタ記憶部２００、方程式生成部２０１、方程式求解部２０２、逆元変換部２０３及び逆元記憶部２０４から

構成される。

逆元演算装置１００は、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクなどから構成されるコンピュータシステムであり、前記ハードディスクには、コンピュータプログラムが記憶されており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作する。これにより、方程式生成部２０１、方程式求解部２０２及び逆元変換部２０３は、それぞれの機能を達成する。

（１）パラメタ記憶部２００

パラメタ記憶部２００は、具体的には、ハードディスクから構成され、生成多項式のパラメタβ、根α、x_0、x_1、・・・、x_{n-1}をあらかじめ記憶している。

（２）方程式生成部２０１

方程式生成部２０１は、パラメタ記憶部２００からパラメタβ、根α、x_0、x_1、・・・、x_{n-1}を読み出し、読み出したパラメタβ、根α、x_0、x_1、・・・、x_{n-1}を用いて、y_i（ｉ＝０、１、２、・・・、ｎ－１）に関する連立方程式

$$
\begin{aligned}
&x_0 y_0 + \beta x_{n-1} y_1 + \beta x_{n-2} y_2 + \cdots + \beta x_1 y_{n-1} = 1 \\
&x_1 y_0 + x_0 y_1 + \beta x_{n-1} y_2 + \cdots + \beta x_2 y_{n-1} = 0 \\
&x_2 y_0 + x_1 y_1 + x_0 y_2 + \cdots + \beta x_3 y_{n-1} = 0 \\
&\qquad\qquad \cdots \\
&x_{n-1} y_0 + x_{n-2} y_1 + x_{n-3} y_2 + \cdots + x_0 y_{n-1} = 0
\end{aligned}
$$

のパラメタを生成する。

【００５１】

前記連立方程式は、次のように表現できる。

ＡＹ＝Ｂ

ここで、

【００５２】

【数１３】

$$\text{行列A}=\begin{pmatrix} x_0 & \beta x_{n-1} & \beta x_{n-2} & \cdots & \beta x_1 \\ x_1 & x_0 & \beta x_{n-1} & \cdots & \beta x_2 \\ x_2 & x_1 & x_0 & \cdots & \beta x_3 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ x_{n-1} & x_{n-2} & x_{n-3} & \cdots & x_0 \end{pmatrix}$$

$$\text{ベクトルY}=\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ \cdot \\ \cdot \\ y_{n-1} \end{pmatrix}$$

$$\text{ベクトルB}=\begin{pmatrix} 1 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ 0 \end{pmatrix}$$

【００５３】

方程式生成部２０１が生成する連立方程式のパラメタは、行列Ａ及びベクトルＢである。方程式生成部２０１は、生成した行列Ａとベクトルとを方程式求解部２０２へ出力する。

また、方程式生成部２０１は、パラメタ記憶部２００から根αを読み出し、読み出した根αを逆元変換部２０３へ出力する。

（３）方程式求解部２０２

方程式求解部２０２は、予め与えられた有限体ＧＦ（ｐ）（ｐは素数）において、以下に示すx_i（ｉ＝１、２、・・・、ｎ）に関するｎ元連立一次方程式のパラメータa_{ij}（ｉ、ｊ＝１、２、・・・、ｎ）、b_k（ｋ＝１、２、・・・、ｎ）が与えられたとき、ｎ元連立一次方程式のＧＦ（ｐ）上の解を算出する。

【００５４】

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1$$
$$a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2$$
$$\cdots$$
$$a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n$$

方程式求解部２０２は、図１に示すように、定数記憶部１０１、方程式変換部１０２、逆元演算部１０３及び方程式演算部１０４から構成される。

（定数記憶部１０１）

定数記憶部１０１は、具体的には、ＲＡＭから構成され、方程式生成部２０１から行列Ｍとベクトルｖとを受け取り、記憶する。ここで、

【００５５】

【数１４】

$$\text{行列M} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

$$\text{ベクトルv} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

【００５６】

ここで、行列Ｍは、一例として、行列Ａであり、ベクトルｖは、一例として、ベクトルＢである。

（方程式変換部１０２）

方程式変換部１０２は、定数記憶部１０１から行列Ｍとベクトルｖとを読み出し、読み出した行列Ｍ及びベクトルｖを三角化変換して、方程式Ｍｘ＝ｖと同値の関係を有するｎ元連立一次方程式Ｍ’ｘ＝ｖ’の行列Ｍ’（Ｍ’はｎ行ｎ列の成分からなる係数行列）及びベクトルｖ’（ｖ’はｎ個の成分からなる定数ベク

トル）を生成する。

【００５７】

前記三角化変換において、方程式変換部１０２は、行列Ｍの各対角成分が１に変換されないように、行列Ｍを上三角行列に変換する。

ここで、

【００５８】

【数１５】

$$\text{行列}M' = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix}$$

$$\text{ベクトル}v' = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix}$$

【００５９】

前記三角化変換について以下に説明する。

前記三角化変換では、方程式Ｍｘ＝ｖから、連続する１個以上の変換過程を介して前記ｎ元連立一次方程式Ｍ’ ｘ＝ｖ’の行列Ｍ’及びベクトルｖ’を生成する。

前記各変換過程において、前記三角化変換手段は、変換前のｎ元連立一次方程式から、変換前のｎ元連立一次方程式と同値の関係を有する変換後のｎ元連立一次方程式の係数行列及び定数ベクトルを生成する。ここで、最初の変換過程において、変換前のｎ元連立一次方程式は、方程式Ｍｘ＝ｖであり、最後の変換過程において、変換後のｎ元連立一次方程式は、方程式Ｍ’ ｘ＝ｖ’である。

【００６０】

前記各変換過程において、前記変換前のｎ元連立一次方程式は、変換の対象と

なる１個以上のｎ元一次方程式である対象方程式と、変換の軸となるｎ元一次方程式である軸方程式とを含む。

前記三角化変換では、前記各変換過程において、前記各対象方程式を、前記対象方程式と同値の関係を有する同値方程式に変換する場合に、第１係数群と第２係数群とを定める。

【００６１】

ここで、前記第１係数群と前記第２係数群とは、それぞれ軸方程式に係る１個以上の値を含む群である。前記対象方程式において、各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引くことにより、前記対象方程式において０でない係数を有する最高次の変数の係数が０となる前記同値方程式が得られる。

【００６２】

前記三角化変換では、前記対象方程式において、０でない係数を有する最高次の変数の係数を０とする。次に、前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引く。

また、前記三角化変換では、前記各変換過程において、１個以上の対象方程式をそれぞれ変換する前記対象方程式と同数の副変換過程とを含む。

【００６３】

前記三角化変換では、各副変換過程において、軸方程式の０でない係数を有する最高次の変数の係数から構成される群を第１係数群と定め、軸方程式の各係数及び定数のそれぞれに対象方程式の０でない係数を有する最高次の変数の係数を乗じ、得られた各値から構成される群を第２係数群と定める。

次に、前記三角化変換では、前記対象方程式において、０でない係数を有する最高次の変数の係数を０とする。また、前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引く。

【００６４】

三角化変換のさらなる詳細については、後述する。

方程式変換部１０２は、生成した行列M’及びベクトルｖ’を方程式演算部１０４へ出力し、生成した行列M’の対角成分c_{ii}（ｉ＝１、２、・・・、ｎ）を逆元演算部１０３へ出力する。

上記に説明するように、方程式変換部１０２は、行列Ｍを上三角行列になるように変換する。このとき、方程式の解を変化させないようにするため、ベクトルｖも変化させている。従来法と異なる点は、対角成分を１にしないことである。

（逆元演算部１０３）

逆元演算部１０３は、方程式変換部１０２から行列M’の対角成分c_{ii}（ｉ＝１、２、・・・、ｎ）を受け取る。

【００６５】

ここで、記述を簡単にするために、行列M’の対角成分c_{ii}（ｉ＝１、２、・・・、ｎ）を、m_i（ｉ＝１、２、・・・、ｎ）と表現する。

逆元演算部１０３は、

【００６６】

【数１６】

$$t_i = \prod_{k=1}^{n} m_k \quad (m_i \text{を除く}) \bmod p$$

$$(i = 1、2、\cdots、n)$$

【００６７】

を次に示すようにして算出する。

逆元演算部１０３は、以下に記載した順序に従って算出する。

$s_1 = m_1 \times m_2 \bmod p$

$s_2 = s_1 \times m_3 \bmod p$

・・・

$s_{n-3} = s_{n-4} \times m_{n-2} \bmod p$

$t_n = s_{n-3} \times m_{n-1} \bmod p$

$t_{n-1} = s_{n-3} \times m_n \bmod p$

$s_n = m_{n-1} \times m_n \mod p$、$t_{n-2} = s_{n-4} \times s_n \mod p$

$s_{n-1} = m_{n-2} \times s_n \mod p$、$t_{n-3} = s_{n-5} \times s_{n-1} \mod p$

$s_{n-2} = m_{n-3} \times s_{n-1} \mod p$、$t_{n-4} = s_{n-6} \times s_{n-2} \mod p$

・・・

$s_5 = m_4 \times s_6 \mod p$、$t_3 = s_1 \times s_5 \mod p$

$s_4 = m_3 \times s_5 \mod p$、$t_2 = m_1 \times s_4 \mod p$

$t_1 = m_2 \times s_4 \mod p$

次に、逆元演算部１０３は、予め与えられたｋ（ｋは、１、２、・・・・、ｎのうちのいずれか１個）を用いて、

$t = t_k \times m_k \mod p$

を算出することにより、

【００６８】

【数１７】

$$t = \prod_{i=1}^{n} m_i \mod p$$

【００６９】

を算出する。

次に、逆元演算部１０３は、

$u = 1 / t \mod p$

を算出する。

次に、逆元演算部１０３は、

逆元$I_i = u \times t_i \mod p$　　（ｉ＝１、２、・・・・、ｎ）

を算出する。

【００７０】

逆元演算部１０３は、算出した逆元I_i（ｉ＝１、２、・・・・、ｎ）を方程式演算部１０４へ出力する。

以上説明したように、逆元演算部１０３は、方程式変換部１０２から出力され

た行列M’の対角成分c_{ii}（ｉ＝１、２、・・・、ｎ）のＧＦ（ｐ）上の逆元Ｉ$_i$（ｉ＝１、２、・・・、ｎ）を計算し、出力する。

（方程式演算部１０４）

方程式演算部１０４は、方程式変換部１０２から行列M’及びベクトルｖ’を受け取り、逆元演算部１０３から逆元Ｉ$_i$（ｉ＝１、２、・・・、ｎ）を受け取る。

【００７１】

方程式演算部１０４は、カウンタｊ＝ｎ－１、ｎ－２、・・・、２、１、０のように設定し、カウンタｊの各値について、行列M’、ベクトルｖ’、逆元Ｉ$_i$（ｉ＝１、２、・・・、ｎ）を用いて、

ｊ＝ｎ－１のとき、　$y_j = I_{j+1} \times d_{j+1} \mod p$

ｊ≠ｎ－１のとき、

【００７２】

【数１８】

$$y_j = I_{j+1} \times \left(d_{j+1} - \sum_{i=j+1}^{n-1} c_{j+1\,i+1} \times y_i \right) \mod p$$

【００７３】

を算出する。

次に、方程式演算部１０４は、算出した解y_j（ｊ＝０、１、２、・・・、ｎ－１）を逆元変換部２０３へ出力する。

以下に、方程式演算部１０４によりｎ元連立一次方程式の解が得られる根拠を示す。

【００７４】

方程式演算部１０４が受け取った行列M’は上三角化行列であるので、方程式M’ｘ＝ｖ’は、

$c_{11}x_0 + c_{12}x_1 + c_{13}x_2 + \ldots + c_{1n}x_{n-1} = d_1$

$$c_{22}x_1 + c_{23}x_2 + \cdots + c_{2n}x_{n-1} = d_2$$
$$\cdots$$
$$c_{nn}x_{n-1} = d_n$$

のように表現でき、行列M'の対角成分c_{ii}（i＝1、2、・・・、n）の逆元は、それぞれI_i（i＝1、2、・・・、n）である。

【００７５】

従って、x_{n-1}の解y_{n-1}は、

$y_{n-1} = I_n \ d_{n-1} \mod p$

である。

次に、x_{n-2}の解y_{n-2}は、

$y_{n-2} = I_{n-1} \ (d_{n-1} - c_{n-1\ n}\ y_{n-1}) \mod p$

である。同様にして、x_jの解y_j（j＝n－3、n－4、・・・、0）は、

【００７６】

【数１９】

$$y_j = I_{j+1} \times \left(d_{j+1} - \sum_{i=j+1}^{n-1} c_{j+1\ i+1} \times y_i\right) \mod p$$

【００７７】

である。

（４）逆元変換部２０３

逆元変換部２０３は、方程式求解部２０２の方程式演算部１０４から解y_j（j＝0、1、2、・・・、n－1）を受け取り、方程式生成部２０１から根αを受け取る。逆元変換部２０３は、受け取った解y_k（j＝0、1、2、・・・、n－1）と根αとを用いて、逆元Iを次の式により演算する。

【００７８】

$I = y_0 + y_1\ \alpha + \cdots + y_{n-1}\ \alpha^{n-1}$

次に、逆元変換部２０３は、算出した逆元Iを逆元記憶部２０４に書き込む。

このようにして、拡大体ＧＦ（ｑ）上の元ｘの逆元Ｉが得られる。

（５）逆元記憶部２０４

逆元記憶部２０４は、具体的にはハードディスクからなり、拡大体ＧＦ（ｑ）上の元ｘの逆元Ｉを記憶する。

１．２　逆元演算装置１００の動作

逆元演算装置１００の動作について説明する。

（１）逆元演算装置１００の全体の概要動作

逆元演算装置１００の全体の概要動作について、図２に示すフローチャートを用いて説明する。

【００７９】

方程式生成部２０１は、パラメタ記憶部２００からパラメタβ、根α、x_0、x_1、・・・、x_{n-1}を読み出し、読み出したパラメタβ、根α、x_0、x_1、・・・、x_{n-1}を用いて、y_i（ｉ＝０、１、２、・・・、ｎ－１）に関する連立方程式ＡＹ＝Ｂのパラメタとして、行列Ａ及びベクトルＢを生成し、生成した行列Ａとベクトルとを方程式求解部２０２の定数記憶部１０１へ出力する（ステップＳ１０１）。

【００８０】

方程式求解部２０２の方程式変換部１０２は、定数記憶部１０１から行列Ｍとベクトルｖとを読み出し、読み出した行列Ｍ及びベクトルｖを三角化変換して、方程式Ｍｘ＝ｖと同値の関係を有するｎ元連立一次方程式Ｍ’ｘ＝ｖ’の行列Ｍ’及びベクトルｖ’を生成する（ステップＳ１０２）。

逆元演算部１０３は、行列Ｍ’の対角成分c_{ii}（ｉ＝１、２、・・・、ｎ）の逆元I_i（ｉ＝１、２、．．．、ｎ）を算出する（ステップＳ１０３）。

【００８１】

方程式演算部１０４は、行列Ｍ’、ベクトルｖ’及び逆元I_i（ｉ＝１、２、・・・、ｎ）を用いて、ｎ元連立一次方程式Ｍ’ｘ＝ｖ’の解y_j（ｊ＝０、１、２、・・・、ｎ－１）を算出し、算出した解を逆元変換部２０３へ出力する（ステップＳ１０４）。

逆元変換部２０３は、方程式求解部２０２から解y_j（ｊ＝０、１、２、・・

・、ｎ－１）を受け取り、方程式生成部２０１から根αを受け取り、、受け取った解と根αとを用いて、拡大体ＧＦ（ｑ）上の元ｘの逆元Ｉを算出し、算出した逆元Ｉを逆元記憶部２０４に書き込む（ステップＳ１０５）。

（２）方程式変換部１０２の三角化変換の詳細の動作

方程式変換部１０２の三角化変換の詳細の動作について、図３に示すフローチャートを用いて説明する。

【００８２】

方程式変換部１０２は、定数記憶部１０１から行列Ｍとベクトルｖとを読み出し（ステップＳ１１１）、カウンタｊを１に設定する（ステップＳ１１２）。

次に、方程式変換部１０２は、行列Ｍの第ｊ列の成分の中でＧＦ（ｐ）上で０でない成分を第ｊ行から第ｎ行まで探索し、はじめに発見した成分の行数をｋとする（ステップＳ１１３）。さらに、ｋ≠ｊの場合に（ステップＳ１１４）、行列Ｍの第ｋ行と第ｊ行とを入れ換え（ステップＳ１１５）、ベクトルｖの第ｋ行と第ｊ行とを入れ換える（ステップＳ１１６）。

【００８３】

次に、方程式変換部１０２は、カウンタｉをｊ＋１に設定し（ステップＳ１１７）、方程式変換部１０２は、a_{jj}（a_{jj}は、行列Ｍのｊ行ｊ列成分）とa_{ij}とを用いて、

$a_{ij}=0$

ｊ＋１≦ｋ≦ｎ（ｋ＝ｊ＋１、ｊ＋２、・・・、ｎ）に対して、

$$a_{ik}=a_{jj}a_{ik}-a_{ij}a_{jk}$$

$$b_i=a_{jj}b_i-a_{ij}b_j$$

のように設定する（ステップＳ１１８）。

【００８４】

方程式変換部１０２は、ｉ＝ｎであるかを判定し、ｉ≠ｎであるなら（ステップＳ１１９）、カウンタｉに１を加算して（ステップＳ１２２）、ステップＳ１１８へ制御を戻す。ｉ＝ｎであるなら（ステップＳ１１９）、ｊ＝ｎ－１であるか判定し、ｊ≠ｎ－１であるなら（ステップＳ１２０）、カウンタｊに１を加算して（ステップＳ１２３）、ステップＳ１１３へ制御を戻す。ｊ＝ｎ－１である

なら（ステップＳ１２０）、行列Ｍを行列Ｍ’とし、ベクトルｖをベクトルｖ’とする。

【００８５】

以上説明したように、方程式変換部１０２には、カウンタｊを変化させることによる変換過程が含まれる。また、前記変換過程内には、カウンタｉを変化させることによる副変換過程が含まれる。

（方程式変換部１０２の検証）

方程式変換部１０２による三角化変換により生成されるｎ元連立一次方程式Ｍ’ｘ＝ｖ’が、ｎ元連立一次方程式Ｍｘ＝ｖと同値の関係を有する根拠をについて以下に説明する。

【００８６】

三角化変換において、ｎ元連立一次方程式中の変換中の１個のｎ元一次方程式について、変換前の行列を行列M_{in}、ベクトルv_{in}とし、変換後の行列を行列M_{out}、ベクトルv_{out}とし、行列M_{in}の第ｉ、ｊ行の行ベクトルをそれぞれ、L_i、L_jとする。

方程式変換部１０２において、

$$a_{jj} \times L_i - a_{ij} \times L_j$$

の計算を行い、この結果の行ベクトルをM_{out}の第ｉ行とし、

$$a_{jj} \times b_i - a_{ij} \times b_j$$

の計算を行い、v_{out}の第ｉ行としている。M_{out}の他の成分及びv_{out}の他の成分は、それぞれM_{in}の他の成分及びv_{in}の他の成分と同じである。このとき、方程式

$$M_{in} \cdot x = v_{in}$$

と方程式

$$M_{out} \cdot x = v_{out}$$

が同じ解をもつことは、「コンピュータによる数値計算」（水上孝一編著、プログラミング入門シリーズ、朝倉書店、1985、76～82ページ）から明らかである。

【００８７】

また、カウンタｊに対して、$j+1 \leqq i \leqq n$を満たすｉについて、a_{ij}を０と

している。この操作をｊが１からｎまで繰り返すので、行列の下三角部分が０になる。したがって、第２方程式変換部１０２は方程式の解を変化させずに、行列の三角化変換が行える。

（３）逆元演算部１０３の動作

逆元演算部１０３の動作について、図４に示すフローチャートを用いて説明する。

【００８８】

逆元演算部１０３は、方程式変換部１０２から行列M’の対角成分m_i（ｉ＝１、２、・・・、ｎ）を受け取り（ステップＳ１４０）、

【００８９】

【数２０】

$$t_i = \prod_{k=1}^{n} m_k \quad (m_i \text{ を除く}) \bmod p \qquad (i = 1、2、\ldots、n)$$

【００９０】

を算出し（ステップＳ１４２）、

予め与えられたｋを用いて、

$t = t_k \times m_k \bmod p$

を算出し（ステップＳ１４３）、

$u = 1 / t \bmod p$

を算出し（ステップＳ１４４）、

逆元$I_i = u \times t_i \bmod p$　　（ｉ＝１、２、．．．、ｎ）

を算出し（ステップＳ１４５）、算出した逆元I_i（ｉ＝１、２、．．．、ｎ）を方程式演算部１０４へ出力する（ステップＳ１４６）。

（４）方程式演算部１０４の動作

方程式演算部１０４の動作について、図５に示すフローチャートを用いて説明する。

【００９１】

方程式演算部１０４は、方程式変換部１０２から行列M'及びベクトルv'を受け取り、逆元演算部１０３から逆元I_i（i＝１、２、・・・、n）を受け取る（ステップＳ１６１）。次に、方程式演算部１０４は、カウンタjをn－１に設定し（ステップＳ１６２）、

j＝n－１のとき、　$y_j = I_{j+1} \times d_{j+1} \mod p$

j≠n－１のとき、

【００９２】

【数２１】

$$y_j = I_{j+1} \times \left(d_{j+1} - \sum_{i=j+1}^{n-1} c_{j+1\,i+1} \times y_i \right) \mod p$$

【００９３】

を算出する（ステップＳ１６３）。

方程式演算部１０４は、j＝０であるか否かを判定し、j＝０であるとき（ステップＳ１６４）、算出した解y_j（j＝０、１、２、・・・、n－１）を逆元変換部２０３へ出力する（ステップＳ１６６）。それ以外の場合は（ステップＳ１６４）、カウンタjから１を減じ（ステップＳ１６５）、ステップＳ１６３へ制御を戻す。

１．３　計算量の評価

方程式求解部２０２における計算量について説明する。

（１）方程式変換部１０２における計算量

カウンタjの値に対して、ループ（図３に示すフローチャートのステップＳ１１３～Ｓ１１９）内の処理の計算量は、次のようになる。

【００９４】

カウンタiの１個の値に対して

（ａ）ステップＳ１１８において、j＋１≦k≦n（k＝j＋１、j＋２、・

・・、ｎ）に対して、$a_{ik}=a_{jj}\times a_{ik}-a_{ij}\times a_{jk}$の計算をする。従って、２回の乗算を（ｎ－（ｊ＋１）＋１）＝（ｎ－ｊ）回行うので、計算量は、２×（ｎ－ｊ）×Mul 。

【００９５】

（ｂ）ステップＳ１１８において、$b_i=a_{jj}\times b_i-a_{ij}\times b_j$ の計算をする。従って、２回の乗算を行うので、計算量は、２Mul 。

カウンタｉは、ｊ＋１～ｎの範囲で変化するので、ループ（ステップＳ１１３～Ｓ１１９）内の計算量は、

（２×（ｎ－ｊ＋１）×Mul ）×（ｎ－（ｊ＋１）＋１）

＝２×（ｎ－ｊ）×（ｎ－ｊ＋１）×Mul

ステップＳ１１２～Ｓ１２０において、カウンタｊは、１～ｎ－１の範囲で変化するので、方程式変換部１０２全体の計算量は、

【００９６】

【数２２】

$$\sum_{j=1}^{n-1}(2\times(n-j)\times(n-j+1))\,Mul$$

$$=2Mul\times\sum_{j=1}^{n-1}j(j+1)$$

$$=2Mul\times\left(\sum_{j=1}^{n-1}j^2+\sum_{j=1}^{n-1}j\right)$$

$$=2Mul\times(1/6\times n(n-1)(2n-1)+1/2\times n(n-1))$$

$$=2Mul\times 1/6\times n(n-1)(2n-1+3)$$

$$=1/3Mul\times n(n-1)(2n+2)$$

$$=2/3\times n(n-1)(n+1)\,Mul$$

【００９７】

（２）逆元演算部１０３における計算量

（ａ）s_1 ～s_{n-3} 及びt_n を求めるために乗算が、ｎ－２回必要であるので、（ｎ－２）Mul

（ｂ）t_{n-1} を求めるために１回の乗算が必要であるので、Mul

（ｃ）s_n とt_{n-2}、s_{n-1} と t_{n-3}、・・・、s_4 とt_2 を求めるために乗算が、２×（ｎ－３）回必要であるので、２×（ｎ－３）×Mul

（ｄ）t_1 を求めるために１回の乗算が必要であるので、Mul

（ｅ）ｔを求めるために１回の乗算が必要であるので、Mul

（ｆ）ｕ＝１／ｔ　ｍｏｄ　ｐを求めるために、１回の逆元演算が必要であるので、Inv

（ｇ）$I_i = u \times t_i$　ｍｏｄ　ｐ　（ｉ＝１，２，．．．，ｎ）を求めるために、ｎ回の乗算が必要であるので、ｎ×Mul

これらを合計すると、

（（ｎ－２）＋１＋２（ｎ－３）＋１＋１＋ｎ）×Mul＋Inv

＝　（４ｎ－５）×Mul＋Ｉｎｖ

（３）方程式演算部１０４における計算量

カウンタｊに対して、ループ内（図５に示すフローチャートのステップＳ１６３～Ｓ１６５）の処理の計算量を見積もる。

【００９８】

ｊ＝ｎ－１のとき、$y_j = I_{j+1} \times d_{j+1}$　ｍｏｄ　ｐ

ｊ≠ｎ－１のとき、

【００９９】

【数２３】

$$y_j = I_{j+1} \times \left(d_{j+1} - \sum_{i=j+1}^{n-1} c_{j+1\,i+1} \times y_i \right) \quad \mathrm{mod}\ p$$

【０１００】

の計算を行うために、１回の乗算（右辺第１項）と（ｎ－（ｊ＋１）＋１）回の

乗算が必要であるので、計算量は　（ｎ－ｊ＋１）×Mul

カウンタｊは、１～ｎの範囲で変化するので、方程式演算部１０４全体の計算量は、

【０１０１】

【数２４】

$$\sum_{j=1}^{n}(n-j+1)\times Mul$$

$$=\sum_{j=1}^{n} j\times Mul$$

$$=1/2\times n(n+1)\times Mul$$

【０１０２】

（４）具体例

具体例を以下に示す。

従来例３と同様に、素数ｐ＝３１、生成多項式ｆ（ｇ）＝g^5-2、ＧＦ（ｑ）の元ｘ＝$5\alpha^4+29\alpha^3+6\alpha^2+19\alpha+17$とする。連立方程式は、従来例３と同様、図６（ａ）に示すようになる。

【０１０３】

次の演算をする。

a_{21} ＝ ０

a_{22} ＝ １７×１７－１９×１０＝６　ｍｏｄ　３１

a_{23} ＝ １７×１０－１９×２７＝２９　ｍｏｄ　３１

a_{24} ＝ １７×２７－１９×１２＝１４　ｍｏｄ　３１

a_{25} ＝ １７×１２－１９×７＝９　ｍｏｄ　３１

b_2 ＝ １７×０－１９×１＝１２　ｍｏｄ　３１

ｊ＝１（ｉ＝２）のとき

連立方程式は、図６（ｂ）に示すようになる。ここで、係数行列４１１の１列２行の成分が０となっている。

【０１０４】

次に、ｊ＝１の処理終了後、連立方程式は、図６（ｃ）に示すようになる。ここで、係数行列４２１の１列３行～５行の成分が０となっている。

次に、ｊ＝２の処理終了後、連立方程式は、図６（ｄ）に示すようになる。ここで、係数行列４３１の２列３行～５行の成分が０となっている。

次に、ｊ＝３の処理終了後、連立方程式は、図６（ｅ）に示すようになる。ここで、係数行列４４１の３列４行～５行の成分が０となっている。

【０１０５】

次に、ｊ＝４の処理終了後、連立方程式は、図６（ｆ）に示すようになる。ここで、係数行列４５１の４列５行の成分が０となっている。

次に、対角成分の逆元演算を行う。

$s_1 = m_1 \times m_2 = 17 \times 6 = 9 \mod 31$

$s_2 = s_1 \times m_3 = 9 \times 17 = 29 \mod 31$

$t_5 = s_2 \times m_4 = 29 \times 6 = 19 \mod 31$

$t_4 = s_2 \times m_5 = 29 \times 30 = 2 \mod 31$

$s_5 = m_4 \times m_5 = 6 \times 30 = 25 \mod 31$

$t_3 = s_1 \times s_5 = 9 \times 25 = 8 \mod 31$

$s_4 = m_3 \times s_5 = 17 \times 25 = 22 \mod 31$

$t_2 = m_1 \times s_4 = 17 \times 22 = 2 \mod 31$

$t_1 = m_2 \times s_4 = 6 \times 22 = 8 \mod 31$

$t = m_1 \times t_1 = 17 \times 8 = 12 \mod 31$

$u = 1 / t = 1 / 12 = 13 \mod 31$　（逆元演算はこの１回のみである。）

$I_1 = u \times t_1 = 13 \times 8 = 11 \mod 31$

$I_2 = u \times t_2 = 13 \times 2 = 26 \mod 31$

$I_3 = u \times t_3 = 13 \times 8 = 11 \mod 31$

$I_4 = u \times t_4 = 13 \times 2 = 26 \mod 31$

$I_5 = u \times t_5 = 13 \times 19 = 30 \mod 31$

次に、方程式を解く。

$y_4 = I_5 \times d_5 = 30 \times 2 = 29 \mod 31$

$y_3 = I_4 \times (d_4 - c_{45} \times y_4)$

$= 26 \times (28 - 2 \times 29) = 26 \mod 31$

$y_2 = I_3 \times (d_3 - c_{34} \times y_3 - c_{35} \times y_4)$

$= 11 \times (1 - 6 \times 26 - 11 \times 29) = 25 \mod 31$

$y_1 = I_2 \times (d_2 - c_{23} \times y_2 - c_{24} \times y_3 - c_{25} \times y_4)$

$= 26 \times (12 - 29 \times 25 - 14 \times 26 - 9 \times 29)$

$= 25 \mod 31$

$y_0 = I_1 \times (d_1 - c_{12} \times y_1 - c_{13} \times y_2 - c_{14} \times y_3 - c_{15} \times y_4)$

$= 11 \times (1 - 10 \times 25 - 27 \times 25 - 12 \times 26 - 7 \times 29)$

$= 12 \mod 31$

（５）方程式求解部２０２全体における計算量

従って、方程式求解部２０２全体における計算量は、

$2/3 \times n(n-1)(n+1)$ Mul

＋ $(4n-5) \times$ Mul ＋ Inv

＋ $1/2 \times n(n+1) \times$ Mul

＝ $1/6(4n^3 + 3n^2 + 23n - 30)$ Mul ＋ Inv

ここで、ｎ＝５、｜ｑ｜＝１６０（｜ｑ｜はｑのビットサイズ）の場合、一般的な計算機では、Ｉｎｖ＝４０Mulであるとすると、方程式求解部２０２における計算量は、１５０×Mulである。

【０１０６】

このように、本発明の方程式求解部２０２による計算量は、従来の方程式求解装置と比較すると、明らかに少なくなる。したがって、連立方程式の求解を少ない計算量で行える有限体上の連立方程式求解装置を提供することができ、この実用的価値は非常に大きい。

また、予め与えられた有限体ＧＦ（ｐ）の拡大体ＧＦ（ｑ）上の元ｘの逆元Ｉを算出する逆元演算装置において、少ない計算量で逆元演算を行うことができる。

（６）適用例

実際に暗号通信システム、デジタル署名通信システム及び誤り訂正通信システムなどの通信システムにおいて、適用される一例としてのパラメタを示す。

【０１０７】

素数$p=2^{31}-1$、$q=p^n$、$n=5$、生成多項式$f(g)=g^5-g-8$

$F(q)$の元$x=x_0+x_1\times\alpha+x_2\times\alpha^2+x_3\times\alpha^3+x_4\times\alpha^4$

に対して、連立方程式は以下のように設定される。

【０１０８】

【数２５】

$$\begin{bmatrix} x_0 & 8x_4 & 8x_3 & 8x_2 & 8x_1 \\ x_1 & x_0+x_4 & x_3+8x_4 & x_2+8x_3 & x_1+8x_2 \\ x_2 & x_1 & x_0+x_4 & x_3+8x_4 & x_2+8x_3 \\ x_3 & x_2 & x_1 & x_0+x_4 & x_3+8x_4 \\ x_4 & x_3 & x_2 & x_1 & x_0+x_4 \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

【０１０９】

ここで、p、x_0、・・・、x_4、y_0、・・・、y_4は、それぞれ３１ビットであり、q、xは、１５５ビットである。

２　その他の実施の形態

本発明に係るその他の実施の形態について説明する。

２．１　変形例

方程式求解部２０２の方程式変換部１０２の変形例としての方程式変換部１０２ａについて説明する。

【０１１０】

方程式変換部１０２ａは、方程式変換部１０２で説明した前記各変換過程において、１個の係数群算出過程と、前記係数群算出過程後に１個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含む。

前記係数群算出過程において、方程式変換部１０２ａは、軸方程式及び１個以上の対象方程式の０でない係数を有する最高次の変数の各係数について、前記各係数を除く他の係数を乗じることにより得られる２個以上の値から構成される群を第１係数群と定め、前記第１係数群に含まれる値であって、軸方程式の０でな

い係数を有する最高次の変数の係数を除く他の係数を乗じることにより得られる値と、軸方程式の各係数及び定数とをそれぞれ乗じ、得られた１個以上の値から構成される群を第２係数群と定める。

【０１１１】

前記副変換過程において、方程式変換部１０２ａは、前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし、前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引く。

【０１１２】

方程式変換部１０２ａの動作について、図７に示すフローチャートを用いて説明する。図７に示すフローチャートは、図３のフローチャートのステップＳ１１８に代えて、ステップＳ１１８ａ～Ｓ１１８ｃを含む。

以下に、ステップＳ１１８ａ～Ｓ１１８ｃについて説明する。他のステップは、図３のフローチャートのステップと同じであるので、説明を省略する。

【０１１３】

方程式変換部１０２ａは、ステップ１１８ａにおいて、ｊ≦ｋ≦ｎなるｋ（ｋ＝ｊ、ｊ＋１、・・・、ｎ）に対して、

【０１１４】

【数２６】

$$h_k = \prod_{m=j}^{n} a_{mj} \quad (a_{kj}\text{除く})$$

【０１１５】

を算出する。

また、方程式変換部１０２ａは、ステップ１１８ｂにおいて、ｊ＋１≦ｋ≦ｎなるｋ（ｋ＝ｊ＋１、ｊ＋２、・・・、ｎ）に対して、

$$w_k = h_j \times a_{jk}$$

$$e = h_j \times b_j$$

を算出する。

【０１１６】

また、方程式変換部１０２ａは、ステップ１１８ｃにおいて、

$a_{ij}=0$とし、

$j+1 \leqq k \leqq n$なるｋ（$k=j+1$、$j+2$、・・・、ｎ）に対して、

$a_{ik}=h_i \times a_{ik}-w_k$を算出し、

$b_i=h_i \times b_i-e$を算出する。

（具体例）

具体例を以下に示す。

【０１１７】

従来例３と同様に、素数ｐ＝３１、生成多項式ｆ（ｇ）＝g^5-2、ＧＦ（ｑ）の元$x=5\alpha^4+29\alpha^3+6\alpha^2+19\alpha+17$とする。連立方程式は、従来例３と同様、図８（ａ）に示すようになる。

ｊ＝１のとき、

$s_1=a_{11} \times a_{21}=17 \times 19=13 \mod 31$

$s_2=s_1 \times a_{31}=13 \times 6=16 \mod 31$

$h_5=s_2 \times a_{41}=16 \times 29=30 \mod 31$

$h_4=s_2 \times a_{51}=16 \times 5=18 \mod 31$

$s_5=a_{41} \times a_{51}=29 \times 5=21 \mod 31$

$h_3=s_1 \times s_5=13 \times 21=25 \mod 31$

$s_4=a_{31} \times s_5=6 \times 21=2 \mod 31$

$h_2=a_{11} \times s_4=17 \times 2=3 \mod 31$

$h_1=a_{21} \times s_4=19 \times 2=7 \mod 31$

を算出し、

$w_2=h_1 \times a_{12}=7 \times 10=8 \mod 31$

$w_3=h_1 \times a_{13}=7 \times 27=3 \mod 31$

$w_4=h_1 \times a_{14}=7 \times 12=22 \mod 31$

$w_5=h_1 \times a_{15}=7 \times 7=18 \mod 31$

$e=h_1 \times b_1=7 \times 1=7 \mod 31$

を算出する。

【０１１８】

次に、ｉ＝２（ｊ＝１）のとき

$a_{21}=0$

$a_{22}=h_2\times a_{22}-w_2=3\times17-8=12 \mod 31$

$a_{23}=h_2\times a_{23}-w_3=3\times10-3=27 \mod 31$

$a_{24}=h_2\times a_{24}-w_4=3\times27-22=28 \mod 31$

$a_{25}=h_2\times a_{25}-w_5=3\times12-18=18 \mod 31$

$b_2=h_2\times b_2-e=3\times0-7=24 \mod 31$

このように、上記の第１の実施形態と異なり、a_{ik}を求めるために、乗算を１回のみ行うので、計算量が少なくなる。（第１の実施形態では、乗算を２回行う。）

こうして、図８（ｂ）に示す連立方程式が得られる。ここで、１列２行の成分が０である。

【０１１９】

次に、ｊ＝１の処理終了後、図８（ｃ）に示す連立方程式が得られる。ここで、１列３行～５行の成分が０である。

次に、ｊ＝２のとき

$s_1=a_{22}\times a_{32}=12\times2=24 \mod 31$

$h_5=s_1\times a_{42}=24\times7=13 \mod 31$

$h_4=s_1\times a_{52}=24\times25=11 \mod 31$

$s_4=a_{42}\times a_{52}=7\times25=20 \mod 31$

$h_3=a_{22}\times s_4=12\times20=23 \mod 31$

$h_2=a_{32}\times s_4=2\times20=9 \mod 31$

を演算し、

$w_3=h_2\times a_{23}=9\times27=26 \mod 31$

$w_4=h_2\times a_{24}=9\times28=4 \mod 31$

$w_5=h_2\times a_{25}=9\times18=7 \mod 31$

$e=h_2\times b_2=9\times24=30 \mod 31$

を演算する。

【０１２０】

次に、ｊ＝２の処理終了後、図８（ｄ）に示す連立方程式が得られる。ここで、２列３行～５行の成分が０である。

次に、ｊ＝３のとき、

$h_5 = a_{33} \times a_{43} = 8 \times 14 = 19 \mod 31$

$h_4 = a_{33} \times a_{53} = 8 \times 12 = 3 \mod 31$

$h_3 = a_{43} \times a_{53} = 14 \times 12 = 13 \mod 31$

を演算し、

$w_4 = h_3 \times a_{34} = 13 \times 1 = 13 \mod 31$

$w_5 = h_3 \times a_{35} = 13 \times 7 = 29 \mod 31$

$e = h_3 \times b_3 = 13 \times 26 = 28 \mod 31$

を演算する。

【０１２１】

次に、ｊ＝３の処理終了後、図８（ｅ）に示す連立方程式が得られる。ここで、３列４行～５行の成分が０である。

次に、ｊ＝４のとき

$h_5 = a_{44} = 16 \mod 31$

$h_4 = a_{54} = 14 \mod 31$

を算出し、

$w_5 = h_4 \times a_{45} = 14 \times 26 = 23 \mod 31$

$e = h_4 \times b_4 = 14 \times 23 = 12 \mod 31$

を算出する。

【０１２２】

次に、ｊ＝４の処理終了後、図８（ｆ）に示す連立方程式が得られる。ここで、４列５行の成分が０である。

ここで、行列Ｃ＝Ａ、ベクトルＤ＝Ｂとする。

次に、対角成分の逆元演算を行う。

$s_1 = m_1 \times m_2 = 17 \times 12 = 18 \mod 31$

$s_2 = s_1 \times m_3 = 18 \times 8 = 20 \mod 31$

$t_5 = s_2 \times m_4 = 20 \times 16 = 10 \mod 31$

$t_4 = s_2 \times m_5 = 20 \times 22 = 6 \mod 31$

$s_5 = m_4 \times m_5 = 16 \times 22 = 11 \mod 31$

$t_3 = s_1 \times s_5 = 18 \times 11 = 12 \mod 31$

$s_4 = m_3 \times s_5 = 8 \times 11 = 26 \mod 31$

$t_2 = m_1 \times s_4 = 17 \times 26 = 8 \mod 31$

$t_1 = m_2 \times s_4 = 12 \times 26 = 2 \mod 31$

$t = m_1 \times t_1 = 17 \times 2 = 3 \mod 31$

$u = 1 / t = 1 / 3 = 21 \mod 31$

を演算する。逆元演算はこの１回のみである。

【０１２３】

$I_1 = u \times t_1 = 21 \times 2 = 11 \mod 31$

$I_2 = u \times t_2 = 21 \times 8 = 13 \mod 31$

$I_3 = u \times t_3 = 21 \times 12 = 4 \mod 31$

$I_4 = u \times t_4 = 21 \times 6 = 2 \mod 31$

$I_5 = u \times t_5 = 21 \times 10 = 24 \mod 31$

を演算する。

【０１２４】

次に方程式を解く。

$y_4 = I_5 \times d_5 = 24 \times 18 = 29 \mod 31$

$y_3 = I_4 \times (d_4 - c_{42} \times y_4)$

$= 2 \times (23 - 26 \times 29) = 26 \mod 31$

$y_2 = I_3 \times (d_3 - c_{34} \times y_3 - c_{35} \times y_4)$

$= 4 \times (26 - 1 \times 26 - 7 \times 29) = 25 \mod 31$

$y_1 = I_2 \times (d_2 - c_{23} \times y_2 - c_{24} \times y_3 - c_{25} \times y_4)$

$= 13 \times (24 - 27 \times 25 - 28 \times 26 - 18 \times 29)$

$= 25 \mod 31$

$y_0 = I_1 \times (d_1 - c_{12} \times y_1 - c_{13} \times y_2 - c_{14} \times y_3 - c_{15} \times y_4)$

＝１１×（１－１０×２５－２７×２５－１２×２６－７×２９）

＝１２　ｍｏｄ　３１

（方程式変換部１０２ａの計算量の評価）

図＊に示すフローチャートにおけるカウンタｊに対するループ内（ステップＳ１１３～ステップＳ１１９）の計算量を見積もる。

【０１２５】

ステップＳ１１８ａにおいて、h_k（ｋ＝ｊ、ｊ＋１、・・・、ｎ）を求めるために、（３×（ｎ－ｊ＋１）－６）回の乗算が必要であるので、計算量は、（３×（ｎ－ｊ＋１）－６）×Mul である。

ステップＳ１１８ｂにおいて、w_k（ｋ＝ｊ＋１、ｊ＋２、・・・、ｎ）とｅとを求めるために、（ｎ－（ｊ＋１）＋１＋１）回の乗算が必要であるので、計算量は、（ｎ－ｊ＋１）×Mul である。

【０１２６】

ステップＳ１１８ｃにおいて、カウンタｉの１個の値に対して、

（ａ）ｊ＋１≦ｋ≦ｎ（ｋ＝ｊ＋１、ｊ＋２、・・・、ｎ）について、$a_{ik}=h_i \times a_{ik}-w_k$の計算をする。１回の乗算を（ｎ－（ｊ＋１）＋１）＝（ｎ－ｊ）回行うので、計算量は（ｎ－ｊ）×Mul である。

（ｂ）$b_i=h_i \times b_i-e$　の計算をする。１回の乗算を行うので、計算量は１Mul である。

【０１２７】

カウンタｉは、ｊ＋１～ｎの範囲で変化するので、ループ内の計算量は、

（（ｎ－ｊ＋１）×Mul）×（ｎ－（ｊ＋１）＋１）

＝（ｎ－ｊ）×（ｎ－ｊ＋１）×Mul

ステップＳ１１８ａ～Ｓ１１８ｃの計算量の合計は、

（（３×（ｎ－ｊ＋１）－６）＋（ｎ－ｊ＋１）＋（ｎ－ｊ）（ｎ－ｊ＋１））×Mul

＝　（４×（ｎ－ｊ＋１）－６＋（ｎ－ｊ）（ｎ－ｊ＋１））×Mul

＝　（（ｎ－ｊ＋４）（ｎ－ｊ＋１）－６）×Mul

カウンタｊは、１～ｎ－１の範囲で変化するので、方程式変換部１０２ａ全体

の計算量は、

【０１２８】

【数２７】

$$\sum_{j=1}^{n-1}((n-j+4)(n-j+1)-6)\,Mul$$

$$=Mul\times\sum_{j=1}^{n-1}((j+4)(j+1)-6)$$

$$=Mul\times\left(\sum_{j=1}^{n-1}j^{2}+5\times\sum_{j=1}^{n-1}j-2\times\sum_{j=1}^{n-1}1\right)$$

$$=Mul\times(1/6\times n(n-1)(2n-1)+5/2\times n(n-1)-2(n-1))$$

$$=Mul\times(1/6\times n(n-1)(2n-1+15)-2(n-1))$$

$$=Mul\times(1/6\times n(n-1)(2n+14)-2(n-1))$$

$$=Mul\times(1/3\times n(n-1)(n+7)-2(n-1))$$

$$=Mul\times(1/3\times(n-1)(n^{2}+7n-6))$$

$$=(1/3\times n^{3}+2n^{2}-13/3\times n+2)\,Mul$$

【０１２９】

従って、方程式求解部全体の計算量は、

$((1/3\times n^{3}+2n^{2}-13/3\times n+2)+(4n-5)+1/2\times n(n+1))\times Mul+Inv$

$=(1/3\times n^{3}+5/2\times n^{2}+1/6\times n-3)\times Mul+Inv$

Inv ＝４０Mul、ｎ＝５と仮定したとき、計算量は、１４２Mul である。

２．２　その他の変形例

（１）ｐを素数、ｑ＝ｐ^{n}、ｎを正の整数、有限体ＧＦ（ｐ）の拡大体ＧＦ（ｑ）上の楕円曲線をＥ、楕円曲線Ｅのベースポイントをｇとし、楕円曲線Ｅ上の離散対数問題を安全性の根拠として利用して、安全性を確保しながら通信する暗号通信システム、デジタル署名通信システム及び誤り訂正通信システムなどの通信システムにおいて、安全性の確保に際して、拡大体ＧＦ（ｑ）上の元の逆元を算出する逆元演算を行う場合に、上記に説明した方程式求解部及び逆元演算装置を適用するようにしてもよい。前記暗号通信システムの一例は、インターネット上でのＥ－ｍａｉｌシステムにおいて、メッセージを暗号化して送受信する場合である。また、デジタル署名通信システムの一例は、電子決済システムである。また、訂正通信システムの一例は、前記Ｅ－ｍａｉｌシステムにおいて、通信回線の品質の悪化等の原因により、送信メッセージの一部が欠落した場合などに、送信メッセージから欠落した部分を検出し、またさらに訂正するシステムである。

【０１３０】

また、前記離散対数問題を安全性の根拠としてデジタル著作物を暗号化し、ＤＶＤ、半導体メモリなどの記録媒体に記録する記録装置において、また、前記暗号化デジタル著作物を復号して再生する再生装置において、暗号又は復号に際して、上記に説明した方程式求解部及び逆元演算装置を適用するようにしてもよい。

【０１３１】

このとき、これらの応用システムにおいて、少ない計算量で逆元演算を行うことができる。

上記の方程式求解部及び逆元演算装置は、例えば、携帯電話機に内蔵されるファームウェア、パソコンに装着される回路基盤として実装されうる。

（２）上記の実施の形態では、$g^{n}-\beta$の形の生成多項式を扱ったが、ｎ次の一般の生成多項式

$$f(g)=\beta_{n}g^{n}+\beta_{n-1}g^{n-1}\cdots+\beta_{2}g^{2}+\beta_{1}g+\beta$$

に対しても同様にして、予め与えられた有限体ＧＦ（ｐ）の拡大体ＧＦ（ｑ）（ｑ＝ｐ^{n}、ｎは正の整数）上の元ｘの逆元Ｉを算出することができる。

【０１３２】

生成多項式をｎ次の一般の多項式ｆ（ｇ）とし、その根をαとする。

拡大体ＧＦ（ｑ）上の元ｘ（$x = x_0 + x_1 \alpha + \cdots + x_{n-1} \alpha^{n-1}$）に対して、（$x \times \alpha^{j-1} \mod f(\alpha)$）の$\alpha^{i-1}$の係数を$a_{ij}$とすると、ｎ元連立一次方程式は、次のように表現できる。

$$a_{11}y_0 + a_{12}y_1 + a_{13}y_2 + \cdots + a_{1n}y_{n-1} = 1$$
$$a_{21}y_0 + a_{22}y_1 + a_{13}y_2 + \cdots + a_{2n}y_{n-1} = 0$$
$$\cdots$$
$$a_{n1}y_0 + a_{n2}y_1 + a_{n3}y_2 + \cdots + a_{nn}y_{n-1} = 0$$

次に、上記のようにｎ元連立一次方程式を表現できる根拠について簡単に説明する。

【０１３３】

$$x \times I = x \times y_0 + x \times y_1 \times \alpha + \cdots + x \times y_{n-1} \alpha^{n-1}$$
$$= 1 \mod f(\alpha)$$

である。

$$x \times y_0 + x \times y_1 \times \alpha + \cdots + x \times y_{n-1} \alpha^{n-1}$$
$$= x \times y_0 + (x \times \alpha \mod f(\alpha)) \times y_1 + \cdots$$
$$+ (x \times \alpha^{n-1} \mod f(\alpha)) \times y_{n-1}$$

であり、α^{i-1}の係数は、

$$a_{i1} \times y_0 + a_{i2} \times y_1 + \cdots + a_{in} \times y_{n-1}$$

で与えられる。

【０１３４】

α^{i-1}（ｉ＞２）の係数は、すべて０であり、α^0（ｉ＝１）の係数は１であるので、上記のｎ元連立一次方程式が得られる。

（３）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

【０１３５】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピーディスク、ハードディスク

、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【０１３６】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を搬送波に載せて、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を搬送波に載せて、前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（４）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【０１３７】

【発明の効果】

以上に説明したように本発明は、有限体ＧＦ（ｐ）（ｐは素数）上のｎ元連立一次方程式Ａｘ＝ｂ（ｎは正の整数、Ａはｎ行ｎ列の成分からなる係数行列、ｘはｎ個の成分からなる変数ベクトル、ｂはｎ個の成分からなる定数ベクトル）の解を求める連立方程式求解装置であって、係数行列Ａと定数ベクトルｂとを記憶しているパラメタ記憶手段と、前記パラメタ記憶手段から係数行列Ａと定数ベクトルｂとを読み出し、読み出した係数行列Ａ及び定数ベクトルｂを三角化変換して方程式Ａｘ＝ｂと同値の関係を有するｎ元連立一次方程式Ｃｘ＝ｄの係数行列Ｃ（Ｃはｎ行ｎ列の成分からなる係数行列）及び定数ベクトルｄ（ｄはｎ個の成分からなる定数ベクトル）を生成する三角化変換手段と、前記三角化変換は、係数行列Ａの各対角成分を１に変換しない、係数行列Ａの上三角行列への変換であり、生成された係数行列Ｃの各対角成分の有限体ＧＦ（ｐ）上の逆元である対角逆元を生成する対角逆元演算手段と、生成された係数行列Ｃと定数ベクトルｄと生成された各対角逆元とを用いて、方程式Ａｘ＝ｂの解として、方程式Ｃｘ＝ｄの解を求める方程式求解手段とを備える。

【０１３８】

この構成によると、連立方程式求解装置の計算量を削減することができる。

ここで、前記三角化変換手段は、連続する１個以上の変換過程を介して前記方程式Ｃｘ＝ｄの係数行列Ｃ及び定数ベクトルｄを生成し、前記各変換過程において、前記三角化変換手段は、変換前のｎ元連立一次方程式から、変換前のｎ元連立一次方程式と同値の関係を有する変換後のｎ元連立一次方程式の係数行列及び定数ベクトルを生成し、最初の変換過程において、変換前のｎ元連立一次方程式は、方程式Ａｘ＝ｂであり、最後の変換過程において、変換後のｎ元連立一次方程式は、方程式Ｃｘ＝ｄであり、前記各変換過程において、前記変換前のｎ元連立一次方程式は、変換の対象となる１個以上のｎ元一次方程式である対象方程式と、変換の軸となるｎ元一次方程式である軸方程式とを含み、前記三角化変換手段は、前記各変換過程において、前記各対象方程式を、前記対象方程式と同値の関係を有する同値方程式に変換する場合に、第１係数群と第２係数群とを定め、ここで、前記第１係数群と前記第２係数群とは、それぞれ軸方程式に係る１個以上の値を含む群であり、前記対象方程式において、各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引くことにより、前記対象方程式において０でない係数を有する最高次の変数の係数が０となる前記同値方程式が得られ、前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし、前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引くように構成してもよい。

【０１３９】

この構成によると、連立方程式の係数行列の対角行列を１としないように、三角化変換が行える。

ここで、前記三角化変換手段は、前記各変換過程において、１個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、前記三角化変換手段は、各副変換過程において、軸方程式の０でない係数を有する最高次の変数の係数から構成される群を第１係数群と定め、軸方程式の各係数及び定数のそれぞれに対象方程式の０でない係数を有する最高次の変数の係数を乗じ、得られた各値から構

成される群を第２係数群と定め、前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし、前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引くように構成してもよい。

【０１４０】

また、前記三角化変換手段は、前記各変換過程において、１個の係数群算出過程と、前記係数群算出過程後に１個以上の対象方程式をそれぞれ変換する同数の副変換過程とを含み、前記係数群算出過程において、前記三角化変換手段は、軸方程式及び１個以上の対象方程式の０でない係数を有する最高次の変数の各係数について、前記各係数を除く他の係数を乗じることにより得られる２以上の値から構成される群を第１係数群と定め、前記第１係数群に含まれる値であって、軸方程式の０でない係数を有する最高次の変数の係数を除く他の係数を乗じることにより得られる値と、軸方程式の各係数及び定数とをそれぞれ乗じ、得られた１個以上の値から構成される群を第２係数群と定め、前記副変換過程において、前記三角化変換手段は、前記対象方程式において、０でない係数を有する最高次の変数の係数を０とし、前記対象方程式において、０でない係数を有する最高次以外の変数の各係数及び定数のそれぞれに前記第１係数群に含まれる値を乗じ、得られたそれぞれの値から前記第２係数群に含まれる値を引くように構成してもよい。

【０１４１】

これらの構成によると、三角化変換において同値の関係を有する方程式を得ることができる。

ここで、係数行列Ｃの対角成分をm_i（ｉ＝１、２、．．．．、ｎ）とし、対角成分m_iのＧＦ（ｐ）上の対角逆元をI_i（ｉ＝１、２、．．．．、ｎ）とし、

前記対角逆元演算手段は、

【０１４２】

【数２８】

$$t_i = \prod_{k=1}^{n} m_k \quad (m_i \text{を除く}) \bmod p$$
$$(i = 1、2、\ldots、n)$$

【０１４３】

を算出し、

【０１４４】

【数２９】

$$t = \prod_{k=1}^{n} m_k \bmod p$$

【０１４５】

を算出する乗算部と、ｕ＝１／ｔ　ｍｏｄ　ｐを算出する第１逆元演算部と、対角逆元I_i　＝　$u \times t_i$　ｍｏｄ　ｐ　（ｉ＝１、２、．．．．、ｎ）を算出する第２逆元演算部とを含むように構成してもよい。

また、前記乗算部は、$s_1 = m_1 \times m_2$　ｍｏｄ　ｐ、$s_2 = s_1 \times m_3$　ｍｏｄ　ｐ、・・・、$s_{n-3} = s_{n-4} \times m_{n-2}$　ｍｏｄ　ｐをこの順序で算出し、次に、$t_n = s_{n-3} \times m_{n-1}$　ｍｏｄ　ｐ、$t_{n-1} = s_{n-3} \times m_n$　ｍｏｄ　ｐ、$s_n = m_{n-1} \times m_n$　ｍｏｄ　ｐ、$t_{n-2} = s_{n-4} \times s_n$　ｍｏｄ　ｐ、$s_{n-1} = m_{n-2} \times s_n$　ｍｏｄ　ｐ、$t_{n-3} = s_{n-5} \times s_{n-1}$　ｍｏｄ　ｐ、$s_{n-2} = m_{n-3} \times s_{n-1}$　ｍｏｄ　ｐ、$t_{n-4} = s_{n-6} \times s_{n-2}$　ｍｏｄ　ｐ、・・・、$s_5 = m_4 \times s_6$　ｍｏｄ　ｐ、$t_3 = s_1 \times s_5$　ｍｏｄ　ｐ、$s_4 = m_3 \times s_5$　ｍｏｄ　ｐ、$t_2 = m_1 \times s_4$　ｍｏｄ　ｐ、$t_1 = m_2 \times s_4$　ｍｏｄ　ｐをこの順序で算出し、次に、正の整数の集合｛１、２、．．．．、ｎ｝から選択された１個の値ｊについて、$t = t_j \times m_j$を算出するように構成してもよい。

【０１４６】

これらの構成によると、対角逆元を算出する演算プロセス内において、逆元演算の回数を削減することができる。

こうして計算量を削減することができ、高速な暗号方式や署名方式を可能にする有限体上の連立方程式求解装置を提供することができ，その実用的価値は大きい。

【０１４７】

また、本発明は、有限体ＧＦ（ｐ）（ｐは素数）の拡大体ＧＦ（ｑ）（ｑ＝p^n、ｎは正の整数）の元ｘの逆元Ｉを演算する逆元演算装置であって、元ｘと拡大体ＧＦ（ｐ）上の多項式の係数とを用いて、ｎ元連立一次方程式Ａｙ＝Ｂの係数行列Ａ及び定数ベクトルＢを生成する方程式生成手段と、上記の連立方程式求解装置であって、ｎ元連立一次方程式Ａｙ＝Ｂの解を求める方程式演算手段と、前記根と求められた前記解とを用いて、逆元Ｉを算出する逆元算出手段とを備える。

【０１４８】

この構成によると、計算量の少ない逆元演算装置を提供することができる。

また、本発明は、有限体ＧＦ（ｐ）（ｐは素数）の拡大体ＧＦ（ｑ）（ｑ＝p^n、ｎは正の整数）の上の楕円曲線をＥ、楕円曲線Ｅのベースポイントをｇとし、楕円曲線Ｅ上の離散対数問題を安全性の根拠として利用して安全性を確保する通信を行い、安全性の確保に際して拡大体ＧＦ（ｑ）上の元ｘの逆元Ｉを算出する通信システムであって、元ｘと拡大体ＧＦ（ｐ）上の多項式の係数とを用いて、ｎ元連立一次方程式Ａｙ＝Ｂの係数行列Ａ及び定数ベクトルＢを生成する方程式生成手段と、上記の連立方程式求解装置であって、ｎ元連立一次方程式Ａｙ＝Ｂの解を求める方程式演算手段と、前記根と求められた前記解とを用いて、逆元Ｉを算出する逆元算出手段とを備える。

【０１４９】

この構成によると、有限体上の逆元演算において計算量の少ない通信システムを提供することができる。

また、本発明は、有限体ＧＦ（ｐ）（ｐは素数）の拡大体ＧＦ（ｑ）（ｑ＝

p^n、ｎは正の整数）の上の楕円曲線をＥ、楕円曲線Ｅのベースポイントをｇとし、楕円曲線Ｅ上の離散対数問題を安全性の根拠として暗号化されたデジタル著作物を記録している記録媒体から暗号化デジタル著作物を読み出して復号し、復号に際して拡大体ＧＦ（ｑ）上の元ｘの逆元Ｉを算出する記録媒体再生装置であって、元ｘと拡大体ＧＦ（ｐ）上の多項式の係数とを用いて、ｎ元連立一次方程式Ａｙ＝Ｂの係数行列Ａ及び定数ベクトルＢを生成する方程式生成手段と、上記の連立方程式求解装置であって、ｎ元連立一次方程式Ａｙ＝Ｂの解を求める方程式演算手段と、前記根と求められた前記解とを用いて、逆元Ｉを算出する逆元算出手段とを備えることを特徴とする。

【０１５０】

この構成によると、有限体上の逆元演算において計算量の少ない記録媒体再生装置を提供することができる。

【図面の簡単な説明】

【図１】

本発明の１の実施の形態としての逆元演算装置１００の構成を示すブロック図である。

【図２】

逆元演算装置１００の全体の動作を示すフローチャートである。

【図３】

逆元演算装置１００の方程式の係数行列の三角化変換の動作を示すフローチャートである。

【図４】

逆元演算装置１００の対角成分の逆元演算の動作を示すフローチャートである。

【図５】

逆元演算装置１００の方程式の演算の動作を示すフローチャートである。

【図６】

方程式変換部１０２を適用する具体例である。

【図７】

方程式変換部１０２ａによる係数行列の三角化変換の動作を示すフローチャートである。

【図８】

変形例としての方程式変換部１０２ａを適用する具体例である。

【図９】

従来のエルガマル署名によるデジタル署名方式の手順を示すシーケンス図である。

【図１０】

従来の係数行列の三角化変換の動作を示すフローチャートである。

【図１１】

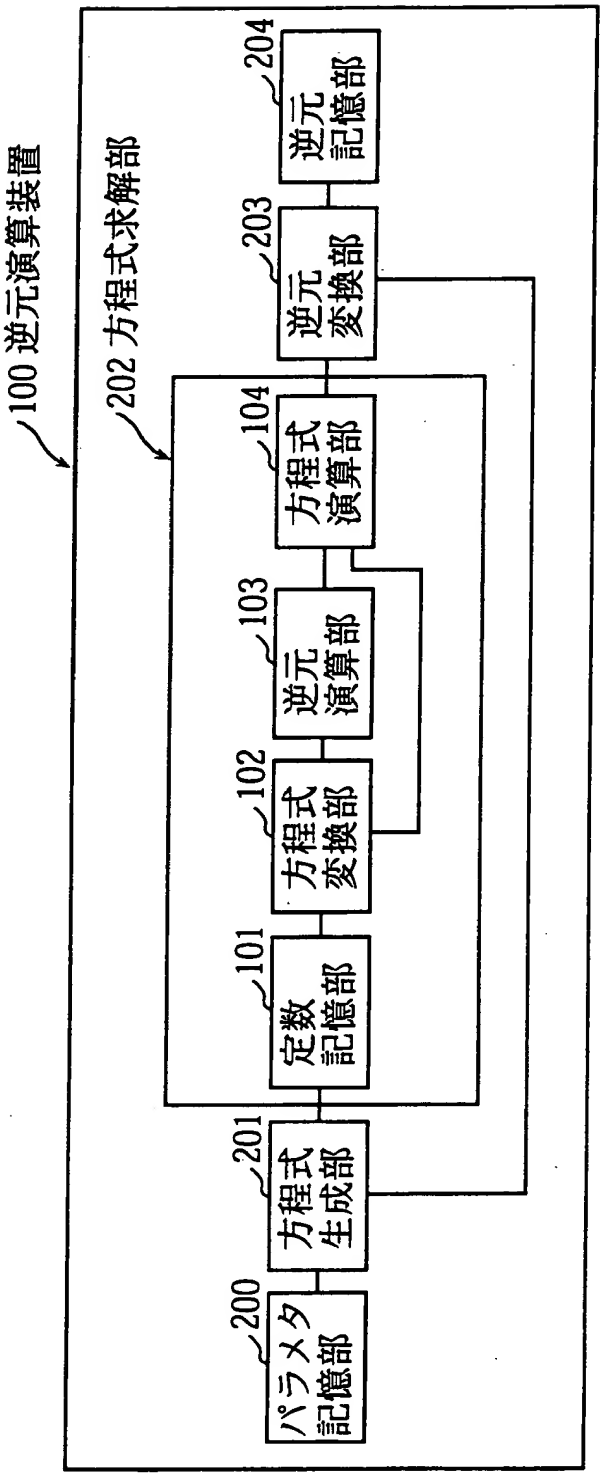
従来の方程式変換を適用する具体例である。

【符号の説明】

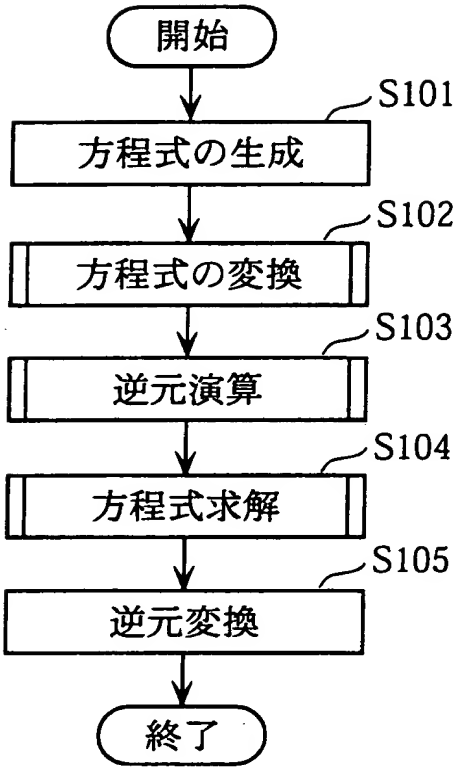
１００	逆元演算装置
１０１	定数記憶部
１０２	方程式変換部
１０２ａ	方程式変換部
１０３	逆元演算部
１０４	方程式演算部
２００	パラメタ記憶部
２０１	方程式生成部
２０２	方程式求解部
２０３	逆元変換部
２０４	逆元記憶部

【書類名】　図面

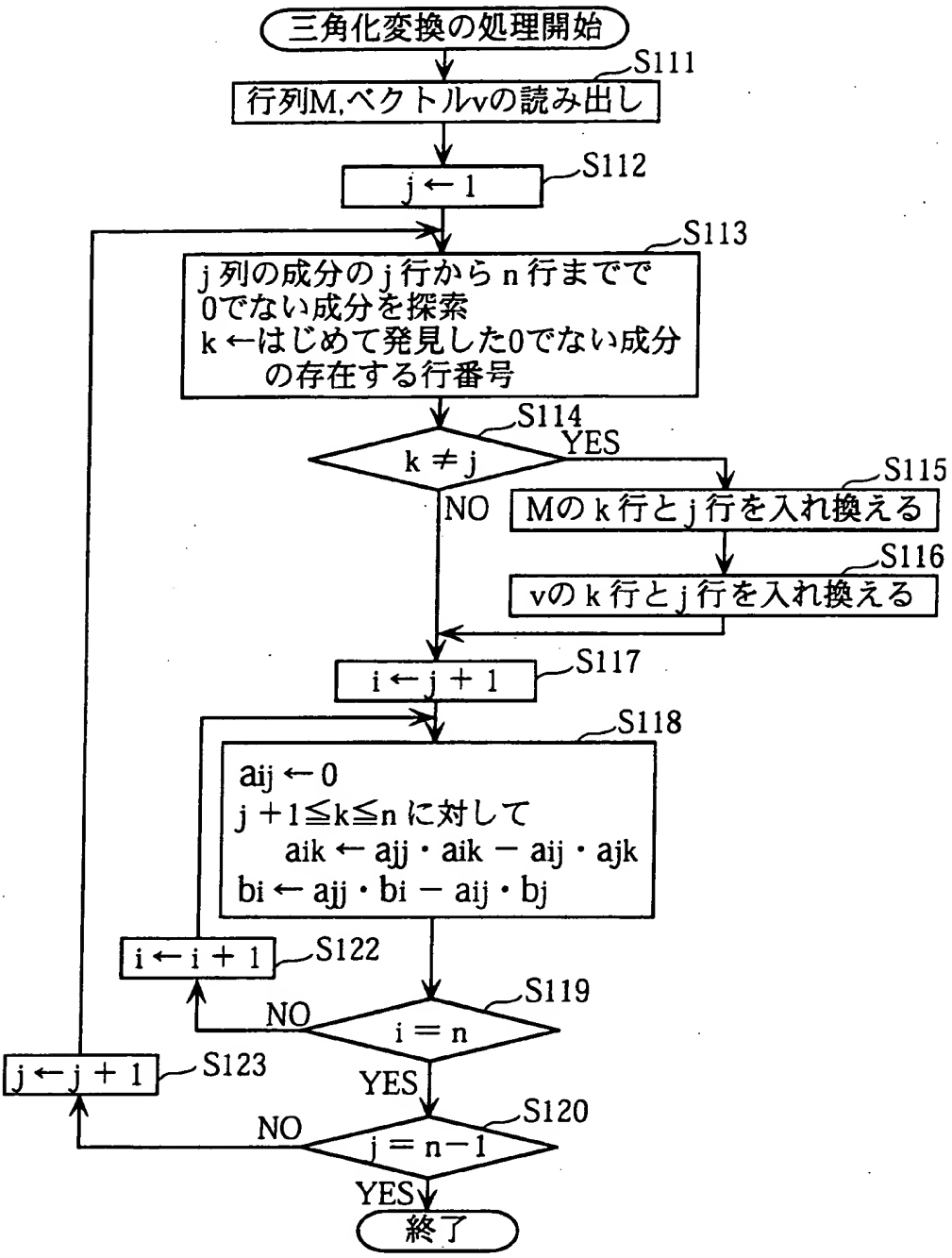
【図１】


100 逆元演算装置
202 方程式求解部
200 パラメタ記憶部
201 方程式生成部
101 定数記憶部
102 方程式変換部
103 逆元演算部
104 方程式演算部
203 逆元変換部
204 逆元記憶部

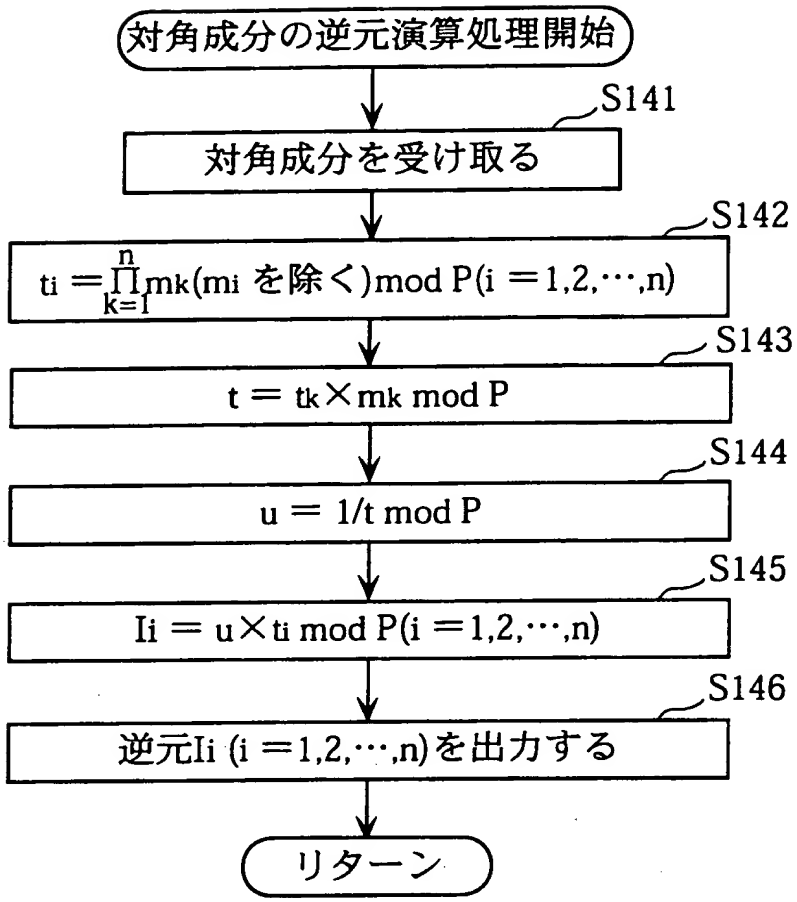
【図２】



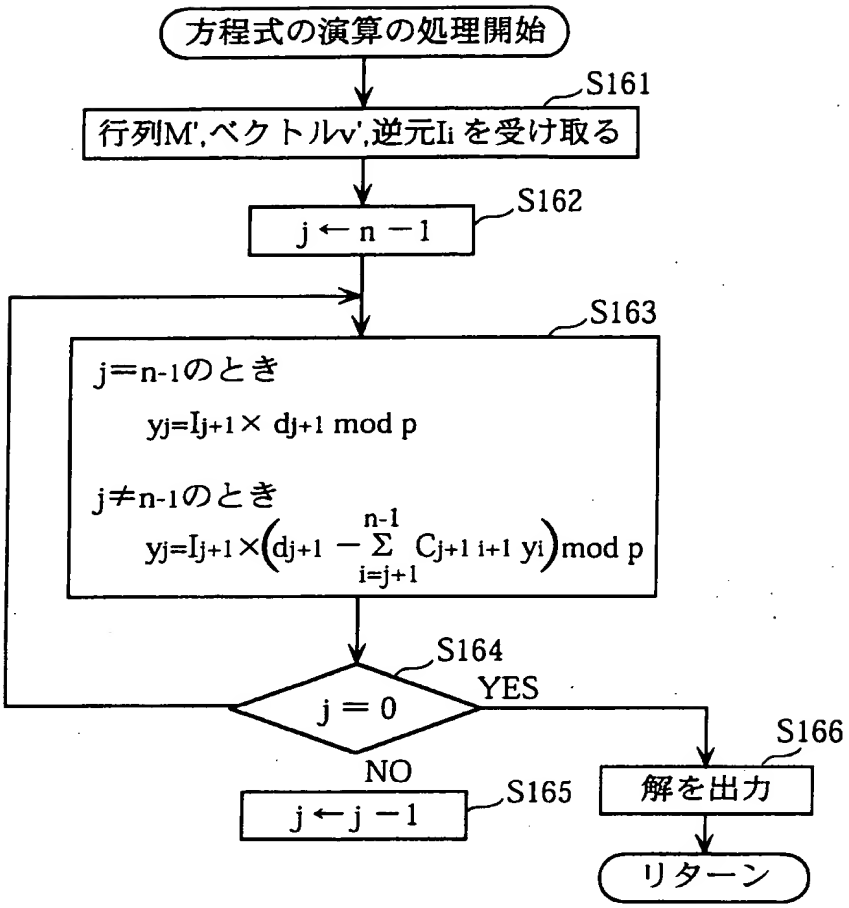
【図３】


三角化変換の処理開始
S111
行列M,ベクトルvの読み出し
S112
j←1
S113
j列の成分のj行からn行までで
0でない成分を探索
k←はじめて発見した0でない成分
の存在する行番号
S114
k≠j
YES
NO
S115
Mのk行とj行を入れ換える
S116
vのk行とj行を入れ換える
S117
i←j＋1
S118
aij←0
j＋1≦k≦nに対して
aik←ajj・aik－aij・ajk
bi←ajj・bi－aij・bj
S122
i←i＋1
S119
NO
i＝n
YES
S123
j←j＋1
S120
NO
j＝n－1
YES
終了

【図４】


対角成分の逆元演算処理開始
S141
対角成分を受け取る
S142
$t_i = \prod_{k=1}^{n} m_k$ (m_i を除く) mod P (i = 1,2,…,n)
S143
t = $t_k \times m_k$ mod P
S144
u = 1/t mod P
S145
$I_i = u \times t_i$ mod P (i = 1,2,…,n)
S146
逆元I_i (i = 1,2,…,n)を出力する
リターン

【図５】


方程式の演算の処理開始
S161
行列M',ベクトルv',逆元Ii を受け取る
S162
j ← n －1
S163
j=n-1のとき
yj=Ij+1× dj+1 mod p
j≠n-1のとき
yj=Ij+1×(dj+1 − Σ Cj+1 i+1 yi) mod p
i=j+1
S164
j = 0
YES
NO
S165
j ← j －1
S166
解を出力
リターン

【図６】

(a)
$$\begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 19 & 17 & 10 & 27 & 12 \\ 6 & 19 & 17 & 10 & 27 \\ 29 & 6 & 19 & 17 & 10 \\ 5 & 29 & 6 & 19 & 17 \end{pmatrix}_{401} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}_{402}$$

(b)
$$\begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ \boxed{0} & 6 & 29 & 14 & 9 \\ 6 & 19 & 17 & 10 & 27 \\ 29 & 6 & 19 & 17 & 10 \\ 5 & 29 & 6 & 19 & 17 \end{pmatrix}_{411} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 1 \\ \boxed{12} \\ 0 \\ 0 \\ 0 \end{pmatrix}_{412}$$

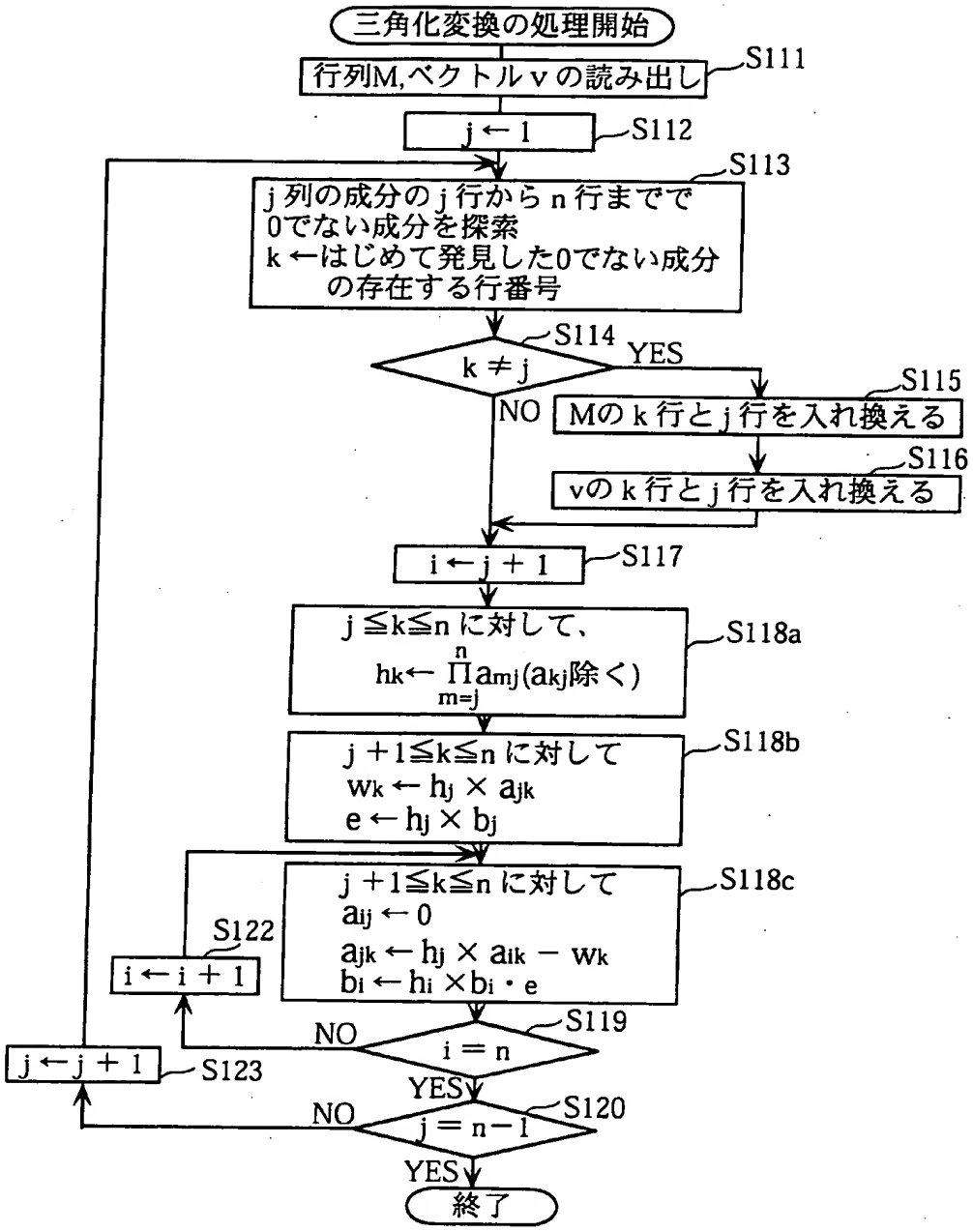
(c)
$$\begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 6 & 29 & 14 & 9 \\ \boxed{0} & 15 & 3 & 5 & 14 \\ \boxed{0} & 29 & 5 & 3 & 29 \\ \boxed{0} & 9 & 29 & 15 & 6 \end{pmatrix}_{421} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 12 \\ \boxed{25} \\ \boxed{2} \\ \boxed{26} \end{pmatrix}_{422}$$

(d)
$$\begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 6 & 29 & 14 & 9 \\ 0 & \boxed{0} & 17 & 6 & 11 \\ 0 & \boxed{0} & 26 & 15 & 6 \\ 0 & \boxed{0} & 6 & 26 & 17 \end{pmatrix}_{431} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 12 \\ \boxed{1} \\ \boxed{5} \\ \boxed{17} \end{pmatrix}_{432}$$

(e)
$$\begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 6 & 29 & 14 & 9 \\ 0 & 0 & 17 & 6 & 11 \\ 0 & 0 & \boxed{0} & 6 & 2 \\ 0 & 0 & \boxed{0} & 3 & 6 \end{pmatrix}_{441} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 12 \\ 1 \\ \boxed{28} \\ \boxed{4} \end{pmatrix}_{442}$$

(f)
$$\begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 6 & 29 & 14 & 9 \\ 0 & 0 & 17 & 6 & 11 \\ 0 & 0 & 0 & 6 & 2 \\ 0 & 0 & 0 & \boxed{0} & 30 \end{pmatrix}_{451} \times \begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \end{pmatrix} = \begin{pmatrix} 1 \\ 12 \\ 1 \\ 28 \\ \boxed{2} \end{pmatrix}_{452}$$

【図７】


三角化変換の処理開始
行列M,ベクトルｖの読み出し
S111
j←1
S112
S113
j列の成分のj行からn行までで
0でない成分を探索
k←はじめて発見した0でない成分
の存在する行番号
S114
k≠j
YES
NO
S115
Mのk行とj行を入れ換える
S116
vのk行とj行を入れ換える
i←j＋1
S117
j≦k≦nに対して、
hk← Π amj(akj除く)
m=j
S118a
j＋1≦k≦nに対して
wk←hj×ajk
e←hj×bj
S118b
j＋1≦k≦nに対して
aij←0
ajk←hj×aik－wk
bi←hi×bi・e
S118c
S122
i←i＋1
NO
S119
i＝n
YES
j←j＋1
S123
NO
S120
j＝n－1
YES
終了

【図８】

(a)
$$\overset{501}{\begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 19 & 17 & 10 & 27 & 12 \\ 6 & 19 & 17 & 10 & 27 \\ 29 & 6 & 19 & 17 & 10 \\ 5 & 29 & 6 & 19 & 17 \end{pmatrix}} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \overset{502}{\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}}$$

(b)
$$\overset{511}{\begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ \boxed{0} & \boxed{12} & \boxed{27} & \boxed{28} & \boxed{18} \\ 6 & 19 & 17 & 10 & 27 \\ 29 & 6 & 19 & 17 & 10 \\ 5 & 29 & 6 & 19 & 17 \end{pmatrix}} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \overset{512}{\begin{pmatrix} 1 \\ \boxed{24} \\ 0 \\ 0 \\ 0 \end{pmatrix}}$$

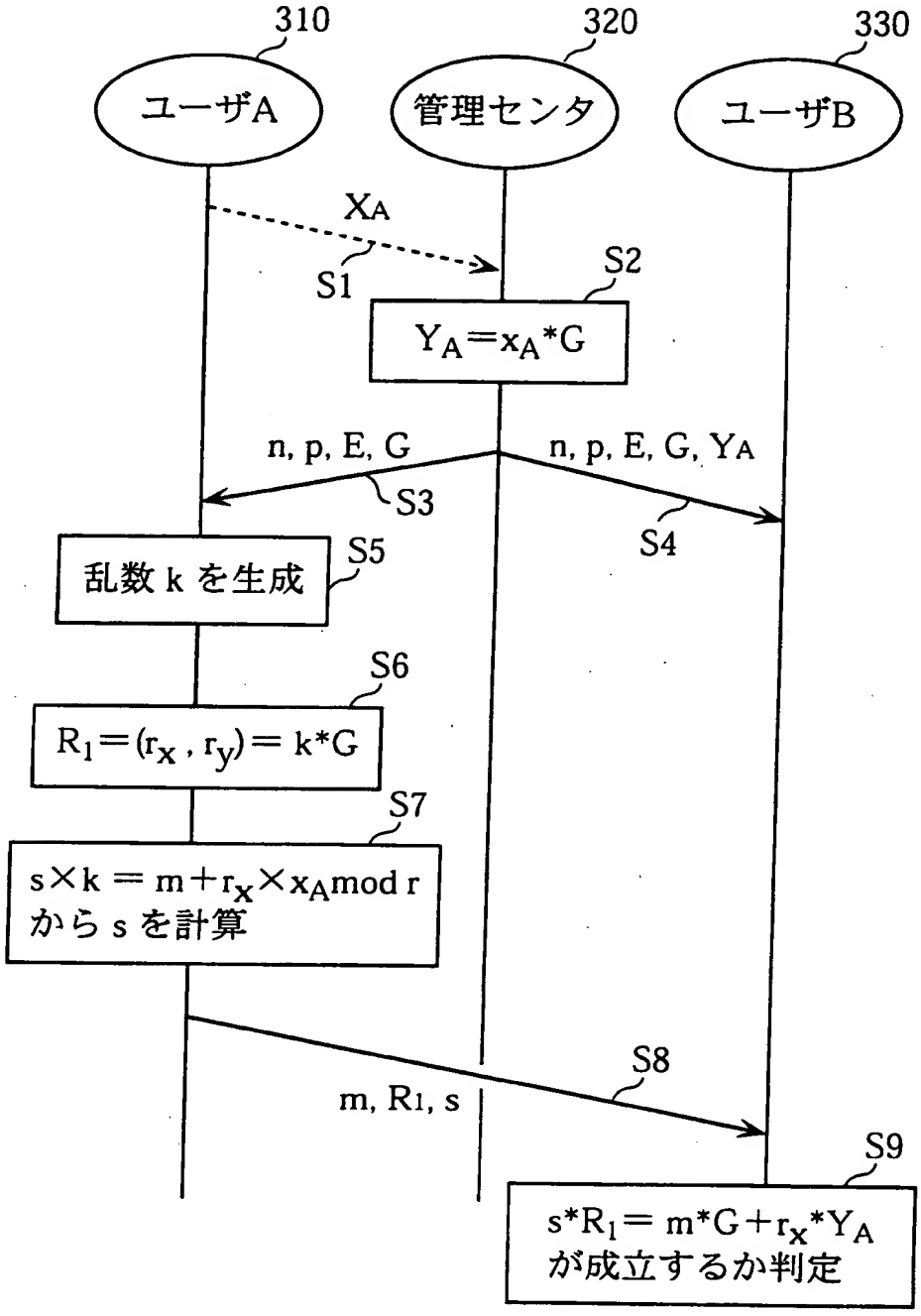
(c)
$$\overset{521}{\begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 12 & 27 & 28 & 18 \\ \boxed{0} & 2 & 19 & 11 & 6 \\ \boxed{0} & 7 & 29 & 5 & 7 \\ \boxed{0} & 25 & 22 & 21 & 27 \end{pmatrix}} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \overset{522}{\begin{pmatrix} 1 \\ 24 \\ \boxed{24} \\ \boxed{24} \\ \boxed{24} \end{pmatrix}}$$

(d)
$$\overset{531}{\begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 12 & 27 & 28 & 18 \\ 0 & \boxed{0} & 8 & 1 & 7 \\ 0 & \boxed{0} & 14 & 20 & 8 \\ 0 & \boxed{0} & 12 & 21 & 3 \end{pmatrix}} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \overset{532}{\begin{pmatrix} 1 \\ 24 \\ \boxed{26} \\ \boxed{17} \\ \boxed{3} \end{pmatrix}}$$

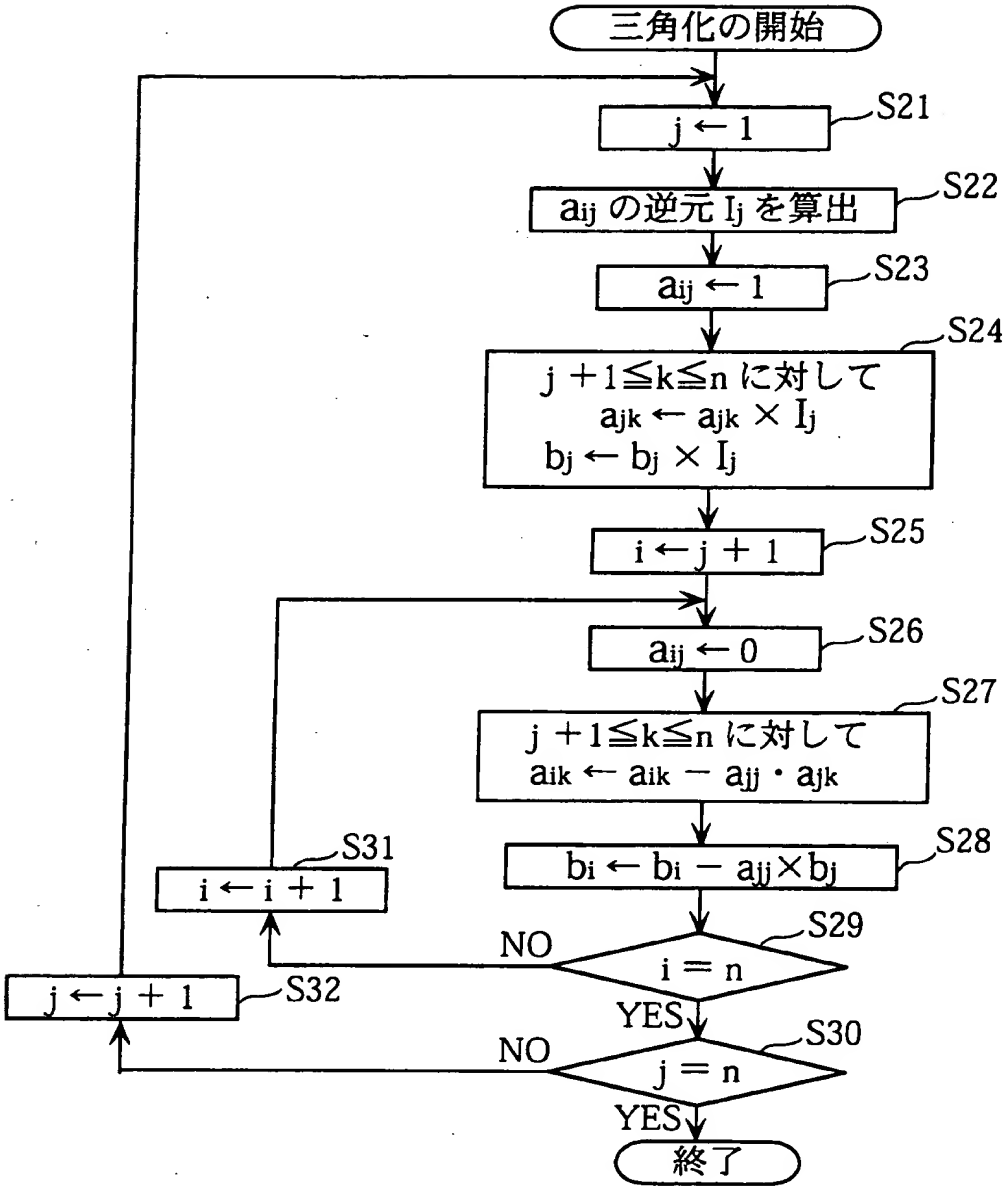
(e)
$$\overset{541}{\begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 12 & 27 & 28 & 18 \\ 0 & 0 & 8 & 1 & 7 \\ 0 & 0 & \boxed{0} & 16 & 26 \\ 0 & 0 & \boxed{0} & 14 & 28 \end{pmatrix}} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \overset{542}{\begin{pmatrix} 1 \\ 24 \\ 26 \\ \boxed{23} \\ \boxed{29} \end{pmatrix}}$$

(f)
$$\overset{551}{\begin{pmatrix} 17 & 10 & 27 & 12 & 7 \\ 0 & 12 & 27 & 28 & 18 \\ 0 & 0 & 8 & 1 & 7 \\ 0 & 0 & 0 & 16 & 26 \\ 0 & 0 & 0 & \boxed{0} & 22 \end{pmatrix}} \times \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} = \overset{552}{\begin{pmatrix} 1 \\ 24 \\ 26 \\ 23 \\ \boxed{18} \end{pmatrix}}$$

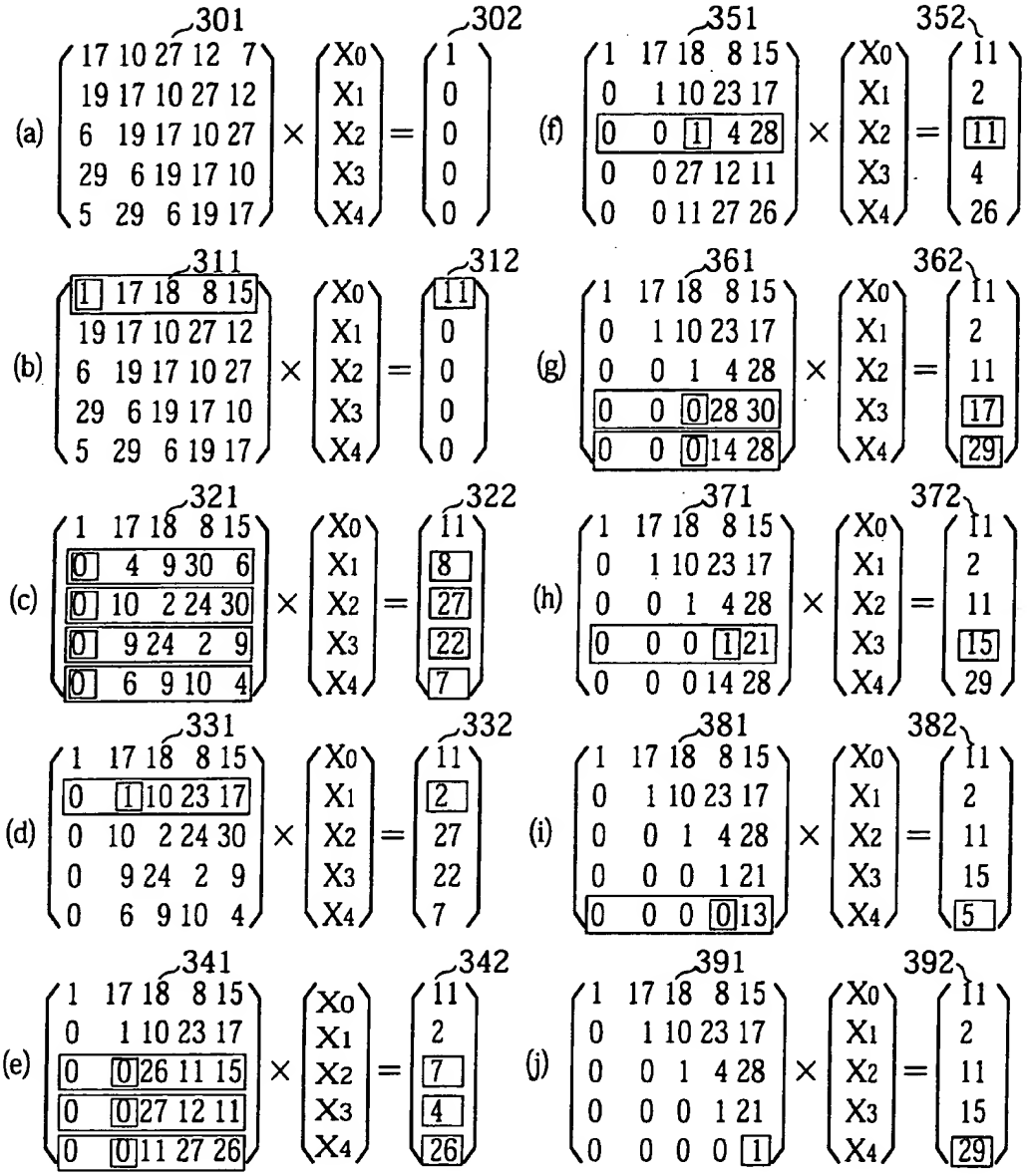
【図９】


310
320
330
ユーザA
管理センタ
ユーザB
XA
S1
S2
YA=xA*G
n, p, E, G
n, p, E, G, YA
S3
S4
乱数 k を生成
S5
S6
R1=(rx , ry)= k*G
S7
s×k = m+rx×xAmod r
から s を計算
S8
m, R1, s
S9
s*R1= m*G+rx*YA
が成立するか判定

【図１０】


三角化の開始
S21
j ← 1
S22
aij の逆元 Ij を算出
S23
aij ← 1
S24
j +1≦k≦n に対して
ajk ← ajk × Ij
bj ← bj × Ij
S25
i ← j + 1
S26
aij ← 0
S27
j +1≦k≦n に対して
aik ← aik − ajj・ajk
S28
bi ← bi − ajj×bj
S29
NO
i = n
YES
S30
NO
j = n
YES
終了
S31
i ← i + 1
S32
j ← j + 1

【図１１】


301
302
(a)
17 10 27 12 7
19 17 10 27 12
6 19 17 10 27
29 6 19 17 10
5 29 6 19 17
X0 X1 X2 X3 X4
1 0 0 0 0
311
312
(b)
1 17 18 8 15
19 17 10 27 12
6 19 17 10 27
29 6 19 17 10
5 29 6 19 17
11 0 0 0 0
321
322
(c)
1 17 18 8 15
0 4 9 30 6
0 10 2 24 30
0 9 24 2 9
0 6 9 10 4
11 8 27 22 7
331
332
(d)
1 17 18 8 15
0 1 10 23 17
0 10 2 24 30
0 9 24 2 9
0 6 9 10 4
11 2 27 22 7
341
342
(e)
1 17 18 8 15
0 1 10 23 17
0 0 26 11 15
0 0 27 12 11
0 0 11 27 26
11 2 7 4 26
351
352
(f)
1 17 18 8 15
0 1 10 23 17
0 0 1 4 28
0 0 27 12 11
0 0 11 27 26
11 2 11 4 26
361
362
(g)
1 17 18 8 15
0 1 10 23 17
0 0 1 4 28
0 0 0 28 30
0 0 0 14 28
11 2 11 17 29
371
372
(h)
1 17 18 8 15
0 1 10 23 17
0 0 1 4 28
0 0 0 1 21
0 0 0 14 28
11 2 11 15 29
381
382
(i)
1 17 18 8 15
0 1 10 23 17
0 0 1 4 28
0 0 0 1 21
0 0 0 0 13
11 2 11 15 5
391
392
(j)
1 17 18 8 15
0 1 10 23 17
0 0 1 4 28
0 0 0 1 21
0 0 0 0 1
11 2 11 15 29

【書類名】　要約書

【要約】

【課題】　有限体上の連立方程式の求解法において、計算量を削減することができる有限体上の連立方程式求解装置を提供する。

【解決手段】　方程式変換部１０２は、行列M及びベクトルｖを三角化変換して、ｎ元連立一次方程式Ｍｘ＝ｖと同値の関係を有する方程式M’ｘ＝ｖ’の行列M’及びベクトルｖ’を生成し、前記三角化変換は、行列Ｍの各対角成分が１に変換されないよう、行列Ｍを上三角行列に変換し、逆元演算部１０３は、行列M’の対角成分の逆元を演算し、方程式演算部１０４は、対角成分の逆元とM’とｖ’とを用いて方程式M’ｘ＝ｖ’の解を算出し、逆元変換部２０３は、解に基づいて有限体ＧＦ（ｐ）の拡大体ＧＦ（ｑ）上の元の逆元Ｉを演算する。

【選択図】　図１

出証特２０００－３０４９５４９

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社